Safeguard Computer Security Evaluation Matrix (SCSEM)

UNIX and Linux

Solaris, HP-UX, AIX, Red Hat Linux, SuSE Linux

Release IV

10-Dec-07

Tester: *Insert Tester Name*
Date: *Insert Date(s) Testing Occured*
Location: *Insert Location testing was conducted*
Agency POC(s): *Insert Agency interviewee(s) names*

Test ID	NIST ID	Test Objective	Test Steps	Expected Results	Actual Results	Pass/ Fail	Comments/ Supporting Evidence
UNIX-LINUX-1	AC-3, AC-6, IA-2, IA-4, IA-5	Checks to see if the UNIX host is bootable in single user mode without a password.	− Solaris 2.5 - 9 # cd /etc/rcS.d # grep sulogin * The sulogin utility should be called from within the svm start up script. Additionally, # more /etc/default/sulogin (if it exists) Confirm PASSREQ=NO is not configured − Solaris 10 # more /etc/default/sulogin (if it exists) Confirm PASSREQ=NO is not configured By default Solaris 10 requires a password and the /etc/default/sulogin does not exist. − HP-UX # more /tcb/files/auth/system/default Confirm the d_boot_authenticate is: :d_boot_authenticate: The entry :d_boot_authenticate@: is a finding. − AIX - AIX has a chassis key that is used to prevent booting to single-user mode without a password. Confirm it is in the correct position and the key has been removed. − Linux - # more /etc/inittab Confirm the following line is configured: ~~:S:wait:/sbin/sulogin	The UNIX host should not allow booting to single user mode without authentication			
UNIX-LINUX-2 (Check only applies if UNIX LINUX-1 is a finding)	AC-3, AC-6, IA-2, IA-4, IA-5, SA-9	Checks to see if the unix host is not configured to require a password when booted to single user mode and is not documented.	Solaris, HP-UX, AIX, and Linux support single-user mode password. If the UNIX host is not be configured to require a password when booted to single-user mode and is not justified and documented with the ISSO, then this is a finding.	The UNIX host is configured to require a password when booted to single-user mode and is justified and documented with the ISSO.			

UNIX-LINUX-3 (Check only applies if UNIX LINUX-1 is a finding)	AC-3, IA-5	The unix host can not be configured to require a password when booted to single user mode and is not located in a controlled access area.	Solaris, HP-UX, AIX, IRIX, and Linux support single-user mode password. − Solaris 2.5 - 9 # cd /etc/rcS.d # grep sulogin * The sulogin utility should be called from within the svm start up script. Additionally, Solaris 10 # more /etc/default/sulogin (if is exists) Confirm PASSREQ=NO is not configured − Solaris 10 # more /etc/default/sulogin (if is exists) Confirm PASSREQ=NO is not configured − HP-UX # more /tcb/files/auth/system/default Confirm the d_boot_authenticate is: :d_boot_authenticate: The entry :d_boot_authenticate@: is a finding. − AIX - AIX has a chassis key that is used to prevent booting to single-user mode without a password. Confirm it is in the correct position and the key has been removed. − Linux - # more /etc/inittab Confirm the following line is configured: ~~:S:wait:/sbin/sulogin If the UNIX host can not be configured to require a password when booted to single-user mode and is not located in a controlled access area accessible only by SAs, then this is a finding. An access-controlled area is defined as requiring two different checks of an individual's identity and authority before gaining access to the system.	The UNIX host can be configured to require a password when booted to single-user mode and is located in a controlled access area accessible only by SAs.			

UNIX-LINUX-4	IA-2, IA-5	Checks to see if password lengths are compliant with IRS requirements of 8 characters or more.	− Solaris Confirm PASSLENGTH is set to 8 or more. # grep PASSLENGTH /etc/default/passwd − HP-UX Confirm MIN_PASSWORD_LENGTH is set to 8 or more # grep MIN_PASSWORD_LENGTH /etc/default/security − AIX Confirm the minlen field is set to 8 or more for each user. # /usr/sbin/lsuser -a minlen ALL − Linux Confirm pass_min_len is set to 8 or more for each user. # grep minlen /etc/pam.d/passwd If a password does not contain a minimum of 8 characters, then this is a finding. If the system does not have the capability to enforce greater than 8 characters, then the password length should be set to 8.	password lengths are compliant with IRS requirements of 8 characters or more.			

UNIX-LINUX-5	IA-2, IA-5	Checks to see if password complexity is enforced when possible depending on the UNIX variant that is deployed.	Verify that at least 2 lowercase letters are required and at least 2 upper case letters. − Solaris 9 and prior This check is not applicable. − Solaris 10 Confirm MINLOWER is set to at least 2 and MINUPPER is set to at least 2. # egrep “MINLOWER|MINUPPER” /etc/default/passwd − HP-UX # grep PASSWORD_MIN_LOWER_CASE_CHARS /etc/default/security # grep PASSWORD_MIN_UPPER_CASE_CHARS /etc/default/security − AIX # grep minalpha /etc/security/user − Linux # egrep lcredit|ucredit /etc/pam.d/system-auth Lcredit and ucredit should be set to -2. If the settings do not enforce at least two lower case letters and two upper case letters, then this is a finding.				

UNIX-LINUX-6	IA-2, IA-5	Checks to see if passwords are changed every 60 days at a minimum.	− Solaris Confirm the max days field (the 5th field) is set to 60 or less, but not 0 for each user. # more /etc/shadow − HP-UX Confirm the exptm is set to 60 or less, but not 0 for each user. # getprpw -r -m exptm <USER> − AIX Confirm the maxage field is set to 60 or less, but not 0 for each user. # /usr/sbin/lsuser -a maxage ALL − Linux Confirm the max days field (the 5th field) is set to 60 or less, but not 0 for each user. # more /etc/shadow If passwords are not changed at least every 60 days, then this is a finding.	Configuration requireds that passwords are changed every 60 days.			
UNIX-LINUX-7	IA-2, IA-5	Checks to see if passwords contain information such as names, telephone numbers, account names, dictionary words, etc.	Interview the SA or ISSO and ask if passwords are allowed that contain contains information such as names, telephone numbers, account names, dictionary words, etc.	Passwords do not contain information such as names, telephone numbers, account names, dictionary words, etc.			
UNIX-LINUX-8	IA-2, IA-5	No automated passwords exist	Interview the ISSO or SA and ask if passwords can be automated through function keys, scripts, or other methods where passwords may be stored on the system.	No automated password methods are used.			

UNIX-LINUX-9	IA-6	Check to see if the feedback from the information system provides information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password is an example of obscuring feedback of authentication information.	Interview ISSO or SA and ask if any applications or services display the user or service account password during input or after authentication.	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.			
UNIX-LINUX-11	SI-2	The ISSO will ensure the operating system is a supported release.	Check the release of the OS: − Solaris # uname -a Supported releases are 2.7 and newer. − HP-UX # uname -a Supported releases are 10.20 and newer. − AIX # uname -a Supported releases are 4.3 and newer, and 5.1 and newer. − Linux # uname -R Supported releases are RedHat Enterprise 3 and newer and SUSE Enterprise 9 and later. If the operating system is not a supported release, then this is a finding.	The operating system is a supported release.			

UNIX-LINUX-12	SI-2	Vendor recommended security patches are not installed or are out of date.	Check installed patches: − Solaris # patchadd –p |grep patch or # showrev –p | grep patch − HP-UX # swlist –l fileset | grep patch − AIX # /usr/sbin/instfix -c -i | cut -d":" -f1 − Linux # RHEL 3 & 4. If using standard Redhat Updates; have the administrator use the up2date -l command to check for new updates. # RHEL 5. If using standard Redhat Updates; have the administrator use the yum check-update command to list available updates. #ALL RHEL cat /etc/redhat-release will provide the maintence release of the installtion. It should be current with the latest maintence patch release. # SUSE SLES-9. Have the administrator use the yast2 utility to check for updates. #ALL If regular updates are being performed, INCLUDING the kernel then the uname -r command can be run to check for kernel updates. Kernel version should be compared to the latest vendor patch list to ensure that it is a supports, secure release. Often this check will indicate if regular patching is occuring. Compare the system output with the most current vendor recommended and security patches. Program managed specific systems should follow their configuration management cycle which may be longer than a normal vendor cycle.	Vendor recommended and security patches are installed and are not out-of-date.			

UNIX-LINUX-13	AC-4,	A non-local non-authoritative time server is used.	Check if NTP running: All platforms # ps –e | egrep “xntpd|ntpd” Check if ntpdate scheduled to run: Solaris # grep ntpdate /var/spool/cron/crontabs/* HP-UX # grep ntpdate /var/spool/cron/crontabs/* AIX # grep ntpdate /var/spool/cron/crontabs/* Linux # grep ntpdate /var/spool/cron/* # grep ntpdate /etc/cron.d/* # grep ntpdate /etc/cron.daily/*I11 # grep ntpdate /etc/cron.hourly/* # grep ntpdate /etc/cron.monthly/* # grep ntpdate /etc/cron.weekly/* If NTP is running or ntpdate is found: # more /etc/ntp/ntp.conf Confirm the servers and peers or multicastclient (as applicable) are local or an authoritative U.S. IRS source. If a non-local/non-authoritative (U.S. IRS approved source) time-server is used, then this is a finding.	An authoritative (U.S. IRS approved source) time-server is used.			
UNIX-LINUX-14	AC-2, IA-2, IA-4	Accounts have the same user or account name.	− Solaris # logins –d − HP-UX # pwck –s − AIX # usrck –n ALL If duplicates are found, perform the following to display full listing. # grep “<account_name>” /etc/passwd − Linux # pwck –r If accounts have the same account name, then this is a finding.	Accounts do not have the same user or account name.			

UNIX-LINUX-15	AC-2, IA-2, IA-4	Accounts have been assigned the same user identification number.	− Solaris # logins –d − HP-UX # pwck –s − AIX # usrck –n ALL If duplicates are found, perform the following to display complete listing. # grep “^.*:.*:<account_uid>” /etc/passwd − Linux # pwck –r If accounts have the same uid, then this is a finding.	Accounts have not been assigned the same uid.			
UNIX-LINUX-16	AC-2, AC-6	The SA will ensure uid’s 0-99 (0-499 Linux) are reserved for system accounts.	# more /etc/passwd # more /etc/passwd Confirm all accounts with a uid of 99 and below (499 and below for Linux) are used by a system account. If a uid reserved for system accounts, 0 – 99 (0 – 499 for Linux), is used by a non-system account without documentation, then this is a finding. A regular account within this range must be justified and documented with the ISSO.	No uid's reserved for system accounts, 0 – 99 (0 – 499 for Linux), are used by a non-system accounts.			
UNIX-LINUX-17	AC-1	An undocumented account exists with a gid of 99 or less.	# more /etc/passwd Confirm all accounts with a gid of 99 and below (499 and below for Linux) are used by a system account. If a gid reserved for system accounts, 0 – 99 (0 – 499 for Linux), is used by a non-system account without documentation, then this is a finding. A regular account within this range must be justified and documented with the ISSO.	No gid's reserved for system accounts are used by a non-system accounts. - gid 14 (sysadmin - Solaris) – may be used if documented with the ISSO. - gid 20 (users - HPUX) – may be used if documented with the ISSO.			

UNIX-LINUX-18	AC-2	A group listed /etc/passwd files is not in the /etc/group file.	Solaris # logins –d HP-UX # pwck –s AIX # grpck Compare with: # more /etc/group Confirm each gid referenced in the /etc/passwd file is listed in the /etc/group file. Linux # pwck –r If a group referenced in the /etc/passwd file is not in the /etc/group file, then this is a finding.	A group referenced in the /etc/passwd file is in the /etc/group file.			

UNIX-LINUX-19	AC-8	The IRS approved login banner is not displayed prior to a login attempt.	Login banners will be configured for all services that allow login access to the system. For TCP WRAPPERS, check for hosts.allow and hosts.deny files and then look for banner files associated with them. For ssh, locate the ssh configuration file, sshd_config or ssh2d_config. This file is usually located in /etc/sshd, /etc/ssh2, /etc/ssh, or /usr/local/etc. Confirm that the Banner variable contains the full path to the file containing the Logon Warning banner. Other files specific to each vendor are listed below. − Solaris: Check for logon warning banner display. # more /etc/issue; # more /etc/motd; # more /etc/dt/config/*/Xresources (if GUI is implemented) # more /etc/default/telnetd (if telnet is implemented without TCP_Wrappers) # more /etc/default/ftpd (if ftp is implemented without TCP_Wrappers) # more /etc/ftpd/banner.msg (Solaris 9 and above, if ftp is implemented without TCP_Wrappers) − HP-UX: Check for logon warning banner display. # more /etc/issue; # more /etc/motd; # more /etc/dt/config/*/Xresources (if GUI is implemented) # more /etc/ftpaccess (if ftp is implemented without TCP_Wrappers – should contain banner=/etc/issue) − AIX: Check for logon warning banner display. # more /etc/motd; # more /etc/dt/config/*/Xresources (if GUI is implemented); # more /etc/ftpmotd; # more /etc/ftpaccess.ctl; # more /dev/console; # more /etc/security/login.cfg − Linux: Check for logon warning banner display. # more /etc/issue; # more /etc/motd; # more /etc/issue.net; # more /etc/X11/xdm/Xresources (if GUI is implemented) # more /etc/X11/xdm/kdmrc (if GUI is implemented); # more /etc/X11/gdm/gdm (if GUI is implemented) # more /etc/vsftpd.conf (if ftp is implemented without TCP_Wrappers) If the IRS logon banner is not displayed prior to a logon attempt, then this is a finding.	The IRS approved login banner is displayed prior to a login attempt. UNAUTHORIZED ACCESS TO THIS UNITED STATES GOVERNMENT COMPUTER SYSTEM AND SOFTWARE IS PROHIBITED BY PUBLIC LAW 99-474, TITLE 18, UNITED STATES CODE. PUBLIC LAW 99-474 AND CHAPTER XXI, SECTION 1030 STATES THAT Whoever knowingly, or intentionally accesses a computer without authorization or exceeds authorized access, and by means of such conduct, obtains, alters, damages, destroys, or discloses information, or prevents authorized use of (data or a computer owned by or operated for) the Government of the United States, shall be punished by a fine under this title or imprisonment for not more than 10 years, or both. All activities on this system may be recorded and monitored. Individuals using this system expressly consent to such monitoring. Evidence of possible misconduct or abuse may be provided to appropriate officials. If the device can only support a short banner, the contents of the banner should be: WARNING! US GOVERNMENT SYSTEM. Unauthorized access prohibited by Public Law 99-474 "The Computer Fraud and Abuse Act of 1986".			
UNIX-LINUX-20	AU-4, 1	Checks to see if the organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	Interview ISSO or SA and ask if log storage is sufficient to meet IRS logging and retention requirements.	Sufficient storage is available to meet IRS logging and retention policies.			

UNIX-LINUX-21	AU-2, AU-3, AU-8	Successful login and logout activity is logged.	− Solaris Check if successful logons are being logged. # last | more Check if unsuccessful logons are being logged. # ls –l /var/adm/loginlog − HP-UX Check if successful logons are being logged. # last –R | more Check if unsuccessful logons are being logged. # lastb –R | more − AIX Check if successful logons are being logged. # last | more Check if unsuccessful logons are being logged. # last –f /etc/security/failedlogin | more − Linux Check if successful logons are being logged. # last –R | more Check if unsuccessful logons are being logged. # lastb –R | more If successful and unsuccessful logins and logouts are not logged, then this is a finding.	Successful and unsuccessful logins and logouts are logged.			

UNIX-LINUX-22	AC-7, AC-9, AC-10	Accounts are disabled after 3 unsuccessful login attempts	− Solaris 5.1 through Solaris 9 Confirm RETRIES is set to 3 or less in /etc/default/login. This does not lock the account, but will discourage brute force password guessing attacks. # grep RETRIES /etc/default/login − Solaris 10 Confirm LOCK_AFTER_RETRIES is set to YES. # grep LOCK_AFTER_RETRIES /etc/security/policy.conf − HP-UX Confirm the u_maxtries is set to 3 or less, but not 0. # grep :u_maxtries# /tcb/files/auth/system/default − AIX Confirm the loginretries field is set to 3 or less, but not 0 for each user. # /usr/sbin/lsuser -a loginretries ALL − Linux # more /etc/pam.d/system-auth Confirm the following line is configured; account required /lib/security/pam_tally.so deny=3 no_magic_root reset If the above settings are not correct, then this is a finding.	After three consecutive unsuccessful login attempts, the account are disabled. (The number of unsuccessful attempts may be determined by the organization)			
UNIX-LINUX-23	AC-7, AC-10, AC-9	The login delay between login prompts after a failed login is set to less than 4 seconds.	− Solaris Confirm SLEEPTIME is set to 4 or more, or that this variable is not configured as 4 is the system default. # grep SLEEPTIME /etc/default/login Note: This check is currently not applicable for Solaris 5.10. − HP-UX Confirm the t_logdelay is set to 4 or more. # grep :t_logdelay# /tcb/files/auth/system/default − AIX Confirm the logindelay field is set to 4 or more. # grep logindelay /etc/security/login.cfg − Linux Confirm FAIL_DELAY is set to 4 or more. # grep FAIL_DELAY /etc/login.defs	The login delay between login prompts after a failed login is set to more than four seconds.			

UNIX-LINUX-24	AC-11, AC-12, SC-10	Determine if automatic session termination applies to local and remote sessions.	The SA will configure systems to log out interactive processes (i.e., terminal sessions, ssh sessions, etc.,) after 15 minutes of inactivity or ensure a password protected screen lock mechanism is used and is set to lock the screen after 15 minutes of inactivity.	Systems are configured to log out of interactive processes (i.e., terminal sessions, ssh sessions, etc.,) after 15 minutes of inactivity or ensure a password protected screen lock mechanism is used and is set to lock the screen after 15 minutes of inactivity.			
UNIX-LINUX-25	AC-5, AC-6, AC-11	The logon session owner for an application requiring a continuous display is root.	If there is an application running on the system that is continuously in use (such as a network monitoring application), ask the SA what the name of the application is. # ps –ef | more If the logon session for an application requiring a continuous display does not ensure: - The logon session is not a root session. - The inactivity exemption is justified and documented with the ISSO. - The display station (e.g., keyboard, CRT) is located in a controlled access area. Then this is a finding.	The logon session for an application requiring a continuous display ensures: - The logon session is not a root session. - The inactivity exemption is justified and documented with the ISSO. - The display station (e.g., keyboard, CRT) is located in a controlled access area.			
UNIX-LINUX-26	AC-2, IA-2, IA-5	Check to see if passwords can be changed more than once every 15 days.	− Solaris Confirm the min days field (the 4th field) is set to 15 or more for each user. # more /etc/shadow − HP-UX Confirm the mintm is set to 15 or more for each user. # getprpw -r -m mintm <USER> − AIX Confirm the minage field is set to 15 or more for each user. # /usr/sbin/lsuser -a minage ALL − Linux Confirm the min days field (the 4th field) is set to 15 or more for each user. # more /etc/shadow If passwords can be changed more than once every 24 hours, then this is a finding.	Passwords cannot be changed more than once every 15 days.			

UNIX-LINUX-27	AC-6, IA-2, IA-4, IA-5,	Check to see if an enabled account on the system is password protected.	Examine the /etc/shadow (or equivalent) looking for accounts with blank passwords using the following commands: SOLARIS # pwck HP-UX # pwck –s or authck –p AIX # pwdck –n ALL Linux # grep nullok /etc/pam.d/system-auth If an entry for nullok is found, then this is a finding on Linux.	An enabled account on the system is password protected.			
UNIX-LINUX-28	AC-2,	Check to see if accounts are locked after 90 days of inactivity.	Indications of inactive accounts are those that have no entries in the last log. Check the date in the last log to verify it is within the last 90 days. If an inactive account is not disabled via an entry in the password field in the /etc/passwd or /etc/shadow (or TCB equivalent), check the /etc/passwd file to check if the account has a valid shell. If not, then this is a finding. Non-interactive application accounts may be documented.	Accounts are locked after 90 days of inactivity			
UNIX-LINUX-29	IA-2, IA-4, IA-5	Check to see if passwords are allowed to be reused within the last 6 changes.	Solaris 10 Confirm HISTORY is set to 6 or more. # grep HISTORY /etc/default/passwd HP-UX # grep HISTORY /etc/default/security Linux # ls /etc/security/opasswd # more /etc/pam.d/system-auth |grep password | grep pam_unix.so | grep remember If /etc/security/opasswd does not exist, then this is a finding. If the 'remember' option in /etc/pam.d/system-auth is not set to 6, then this is a finding. If passwords are reused within the last six changes, then this is a finding.	Passwords are not allowed reused within the last six changes.			

UNIX-LINUX-30	IA-2, IA-4, IA-5	Check to see if global password configuration files are configured per guidelines.	− Solaris Confirm MINWEEKS is set to 2 or more. # grep MINWEEKS /etc/default/passwd Confirm MAXWEEKS is set to 12 or less, but not 0. # grep MAXWEEKS /etc/default/passwd Confirm WARNWEEKS is set to 2 or less. # grep WARNWEEKS /etc/default/passwd +D28− HP-UX Confirm the default mintm is set to 2 or more # getprdef -r -m mintm Confirm the default exptm is set to 90 or less, but not 0 # getprdef -r -m exptm Confirm the default expwarn is set to 14 # getprdef -r -m expwarn − AIX Confirm the following: # grep minage /etc/security/user Should be set to 2 (14 days) # grep maxage /etc/security/user Should be set to 12 (84 days) # grep pwdwarntime /etc/security/user Should be set to 14 (2 Weeks) − Linux Confirm PASS_MIN_DAYS is set to 2 or more. # grep PASS_MIN_DAYS /etc/login.defs Confirm PASS_MAX_DAYS is set to 90 or less, but not 0. # grep PASS_MAX_DAYS /etc/login.defs Confirm PASS_WARN_DAYS is set to 14 #grep PASS_WARN_DAYS /etc/login.defs If global password configuration files are not configured per guidelines, then this is a finding.	Global password configuration files are configured per guidelines.			
UNIX-LINUX-31	IA-2	Check to see if an account other than root has a uid of zero.	grep “:0:” /etc/passwd | awk –F”:” ‘{print$1”:”$3”:”}’ | grep “:0:” If any accounts are shown in addition to root, then this is a finding.	Accounts other than root do not have a uid of 0.			
UNIX-LINUX-32	AC-3, AC-6	Check to see if the root accounts home directory (other than /) is more permissive than 700.	Perform the following as root: # grep “^root” /etc/passwd | awk –F”:” ‘{print $6}’ # ls –ld <root home directory> If the permissions of the root home directory are greater than 700, then this is a finding. If the home directory is /, this check should be marked Not Applicable.	The root account home directory (other than ‘/’) is not more permissive than 700.			

UNIX-LINUX-33	AC-3, AC-6	Checks to see if the root account has world writeable directories in its search path.	As the root user perform the following to check the search path: # echo $PATH # ls –ld <each directory in path variable> If any of the directories in the PATH variable are world writeable, then this is a finding.	The root account does not have world writable directories in its search path.			
UNIX-LINUX-34	AC-6, IA-2, IA-4	Check to see if the root account can be directly logged into from other than the system console.	Solaris Confirm CONSOLE is set to /dev/console. # grep CONSOLE=/dev/console /etc/default/login HP-UX Confirm /etc/securetty exists and is empty or contains only the word console or /dev/null. # more /etc/securetty AIX # /user/sbin/lsuser –a rlogin root Linux Confirm /etc/securetty exists and is empty or contains only the word console or a single tty device. # more /etc/securetty	The root account cannot be directly logged into from somewhere other than the system console.			
UNIX-LINUX-35	AC-17	There are remote consoles defined.	Solaris 2.5, 2.6, and 7 Confirm CONSOLE is set to /dev/console. # grep CONSOLE=/dev/console /etc/default/login Solaris 8, 9, and 10 Confirm there is no output from the below mentioned command. # consadm –p HP-UX Confirm /etc/securetty exists and is empty or contains only the word console or /dev/null. # more /etc/securetty AIX Ensure /etc/security/login.cfg does not define an alternate console. # more /etc/security/login.cfg Linux Confirm /etc/securetty exists and is empty or contains only the word console or a single tty device. # more /etc/securetty	There are no remote consoles defined.			

UNIX-LINUX-36	AC-3, AC-5, AC-6, IA-2, IA-4	Check to see if the root account is logged onto directly.	Perform the following to check if root is logging in directly: # last root |grep –v reboot If any entries exist for root other than the console, then this is a finding.	The root account is not logged onto directly.			
UNIX-LINUX-37	AC-3, AU-2, AU-3, AU-8	Successful and unsuccessful accesses to the root account are not logged.	Check the following log files to determine if access to the root account is being logged. Try to su – and enter an incorrect password. − Solaris # more /var/adm/sulog − HP-UX # more /var/adm/sulog − AIX # more /var/adm/sulog − Linux # more /var/log/messages or # more/var/adm/sulog (configurable from /etc/default/su) If root login accounts are not being logged, then this is a finding.	Successful and unsuccessful access to the root account are logged.			

UNIX-LINUX-38	AC-4, IA-2, IA-4, IA-5	Check to see if the root password is passed over a network in clear text form.	Perform the following to determine if root has logged in over an unencrypted network connection. The first command determines if root has logged in over a network. The second will check to see if ssh is installed. − Solaris # last | grep "^root " | egrep –v "reboot|console" | more # ps –ef |grep sshd − HP-UX # last –R | grep "^root " | egrep –v "reboot|console" | more # ps –ef |grep sshd − AIX # last | grep "^root " | egrep –v "reboot|console" | more # ps –ef |grep sshd − Linux # last | grep "^root " | egrep –v "reboot|console" | more # ps –ef |grep sshd If the output from the 'last' command shows root has logged in over the network and sshd is not running, then this is a finding.	The root password is not passed over a network in clear text form.			
UNIX-LINUX-39	AC-3, AC-6	Check to see if an encrypted remote access program such as ssh is configured to disable the capability to log on directly as root.	Perform the following to determine if ssh disables root logins: # find / -name sshd_config –print # grep -I <sshd_config path> permitrootlogin RHEL 4-5, SLES 9 The permitrootlogins value should be uncommented and set to no. Note: Speak with the administrator regarding alternative ways of restricting direct root ssh logins with PAM if they suggest that root logins via ssh are disabled and the above check suggests otherwise.	An encrypted remote access program, such as ssh, disables the capability to log directly on as root.			

UNIX-LINUX-40	AC-3, AC-6	Check to see if there are files or directories with uneven access permissions.	Perform: # ls –lL <system directory> <system files directories are listed below> to check the permissions for files in /etc, /bin, /usr/bin, /usr/lbin, /usr/usb, /sbin, and /usr/sbin. Uneven file permission exist if the file owner has less privileges than the group or world users and when the file is owned by a privileged user or group (such as root or bin).. If any of the files in the above listed directories contain uneven file permissions, then this is a finding.	There are no files or directories with uneven access permissions.			
UNIX-LINUX-41	AC-3	Check to see if there are unowned files.	Perform: # find / nouser print > nousers and # find / -nogroup –print > nogroup If there are any files listed either in the nousers or nogroup files created from the above commands, then this is a finding.	There are no unowned files.			
UNIX-LINUX-42	AC-3, AC-6	Check to see if network services daemon file permissions are more permissive than 755.	Perform the following to check the permissions: − Solaris # ls –la /usr/bin or /usr/sbin − HP-UX # ls –la /usr/lbin − AIX # ls –la /usr/sbin − Linux # ls –la /usr/sbin If any of the files that are used to start network daemons in the above directories have permissions greater than 755, then this is a finding. Note: Network daemons that may not reside in these directories (such as httpd or sshd) must also be checked for the correct permissions.	Network services daemon file is not more permissive than 755.			

UNIX-LINUX-43	AC-3, AC-6	Check to see if system command permission are more permissive than 755.	Perform: # ls –lL <system directory> <system files directories are listed below> to check the permissions for files in /etc, /bin, /usr/bin, /usr/lbin, /usr/usb, /sbin, and /usr/sbin. If the file permissions are greater than 755, and the files are system commands, then this is a finding. Note: Elevate to Criticality Code of HIGH if world writable.	System command is not more permissive than 755.			
UNIX-LINUX-44	AC-3, AC-6	Check to see if system files, programs, and directories are not owned by a system account.	Perform: # ls –lL <system directory> <system files directories are listed below> to check the owner for files in /etc, /bin, /usr/bin, /usr/lbin, /usr/usb, /sbin, and /usr/sbin. If the files are not owned by a system account or application, then this is a finding.	System files, programs, and directories are owned by a system account.			
UNIX-LINUX-45	AC-3, AC-5, AC-6	Check to see if the group owner of system files, programs, or directories is not a system group.	Perform: # ls –lL <system directory> <system files directories are listed below> to check the group owner for files in /etc, /bin, /usr/bin, /usr/lbin, /usr/usb, /sbin, and /usr/sbin. If the files are not owned by a system group or application group, then this is a finding.	System files, programs, and directories are owned by a system group.			
UNIX-LINUX-46	AC-3, AC-6, AU-9	Check to see if system log file permissions are more permissive than 640.	Most syslog messages are logged to /var/log, /var/log/syslog, or /var/adm directories. Check the permissions by performing the following: # ls –lL <syslog directory> If any of the log files permissions are greater than 640, then this is a finding.	System log file is not more permissive than 640.			
UNIX-LINUX-47	AC-3, AC-6,	Check to see if manual page file permissions are more permissive than 644.	Check the man pages permissions by performing the following: # ls –lL /usr/share/man # ls –lL /usr/share/info # ls –lL /usr/share/infopage If any files in the above directories have permissions greater than 644, then this is a finding.	Manual page file is not more permissive than 644.			

UNIX-LINUX-48	AC-3, AC-6	Library file permissions are more permissive than 755.	Check the library permissions by performing the following: # ls –lL /usr/lib/* If any of the file permissions are greater than 755, then this is a finding.	Library file is not more permissive than 755.			
UNIX-LINUX-49	AC-3,AC-5, AC-6	NIS/NIS+/yp files are not owned by root, sys, or bin.	Perform the following to check NIS file ownership: − Solaris # ls –la /usr/lib/netsvc/yp − HP-UX # ls –la /var/yp/<nis domainname> − AIX # ls –la /usr/lib/netsvc/yp or /usr/lib/nis − Linux # ls –la /var/yp/<nis domainname> If the file ownership is not root, sys, bin, then this is a finding.	NIS/NIS+/yp files are owned by root, sys or bin.			
UNIX-LINUX-50	AC-5, AC-6	The group owner of NIS/NIS+ files is not root, sys, or bin.	Perform the following to check NIS file group ownership: − Solaris # ls –la /usr/lib/netsvc/yp − HP-UX # ls –la /var/yp/<nis domainname> − AIX # ls –la /usr/lib/netsvc/yp or /usr/lib/nis − Linux # ls –la /var/yp/<nis domainname> If the file group ownership is not root, sys, bin or other, then this is a finding.	NIS/NIS+/yp files are group owned root, sys, bin, or other.			

UNIX-LINUX-51	AC-3, AC-6,	NIS/NIS+ command file permissions are more permissive than 755.	Perform the following to check NIS file permissions: − Solaris # ls –la /usr/lib/netsvc/yp − HP-UX # ls –la /var/yp/<nis domainname> − AIX # ls –la /usr/lib/netsvc/yp or /usr/lib/nis − Linux # ls –la /var/yp/<nis domainname> If any of the file permissions are greater than 755, then this is a finding.	NIS/NIS+/yp command file is not more permissive than 755.			
UNIX-LINUX-52	AC-3, AC-6	Checks to see if the /etc/passwd file protection is more permissive than 644.	Check /etc/passwd permissions: # ls –lL /etc/passwd If /etc/passwd is more permissive than 644, then this is a finding.	The /etc/passwd file is not more permissive than 644.			

UNIX-LINUX-53	AC-3, AC-6	Checks to make sure that the /etc/passwd file is not owned by root.	Check /etc/passwd ownership: # ls –lL /etc/passwd Check /etc/shadow and equivalent file(s) ownership: − HP-UX The TCB structure of HP-UX and other flavors of UNIX is radically different from the /etc/shadow structure found in Solaris. The file permissions and uids/gids should be as follows, and are a finding if they deviate from this configuration. /tcb d555 root sys /tcb/files d771 root sys /tcb/files/auth d771 root sys /tcb/files/auth/[a-z]/* 664 root root − AIX. # ls –lL /etc/security/passwd − All Other Platforms # ls –lL /etc/shadow If the /etc/passwd and /etc/shadow (or equivalent) file is not owned by root, then this is a finding. If HP-UX /tcb directories and files ownerships are not configured as detailed above, then this is a finding.	The /etc/passwd and /etc/shadow (or equivalent) file is owned by root			

UNIX-LINUX-54	AC-3, AC-6	Checks to see if the shadow file permissions are more permissive than 400.	Check /etc/shadow and equivalent file(s) permissions: − HP-UX The TCB structure of HP-UX and other flavors of UNIX is radically different from the /etc/shadow structure found in Solaris. The file permissions and uids/gids should be as follows, and are a finding if they deviate from this configuration. /tcb d555 root sys /tcb/files d771 root sys /tcb/files/auth d771 root sys /tcb/files/auth/[a-z]/* 664 root root − AIX. # ls –lL /etc/security/passwd − All Other Platforms # ls –lL /etc/shadow If the /etc/shadow (or equivalent) file is more permissive than 400, then this is a finding. If HP-UX /tcb directories and files permissions are not configured as detailed above, then this is a finding.	The /etc/shadow (or equivalent) file is not more permissive than 400.			
UNIX-LINUX-55	AC-3, AC-6	Checks to see if home directories have permissions greater than 750.	Issue this command for each user in the /etc/passwd file to display user home directory permissions: # ls –lLd /<usershomedirectory> If a user's home directories are more permissive the 750, then this is a finding. Home directories with permissions greater than 750 must be justified and documented with the ISSO.	User home directories are not more permissive than 750.			
UNIX-LINUX-56	AC-3, AC-6	Checks to see if users do own their home directory.	Issue this command for each user in the /etc/passwd file to display user home directory ownership: # ls –lLd /<usershomedirectory> If a user's home directory(s) are not owned by the assigned user, then this is a finding. Home directories not owned by the assigned user must be justified and documented with the ISSO.	Users own their home directory.			

UNIX-LINUX-57	AC-3	Checks to see if an accounts primary gid is different from the account home directory gid.	Issue this command for each user in the /etc/passwd file to display user home directory group ownership: # ls –lLd /<usershomedirecotory> # grep <user> /etc/group If user home directories are not group owned by the assigned user's primary group, then this is a finding. Home directories with a group owner other than the assigned owner must be justified and documented with the ISSO.	Home directories are group owned by the home directory owner's primary group. Exceptions may exist for application directories, which will be documented with the ISSO.			
UNIX-LINUX-58	AC-3,AC-5, AC-6	Checks to see if system start-up files are more permissive than 755.	Check run control scripts permissions: − Solaris # cd /etc # ls –lL rc* # cd /etc/init.d # ls –l − HP-UX # cd /sbin # ls –lL rc* # cd /sbin/init.d # ls –l # /etc/rc.config.d # ls -l − AIX # cd /etc # ls –lL rc* − Linux # cd /etc (may vary) # ls –lL rc* # cd /etc/init.d # ls –l If run control scripts are more permissive than 755, then this is a finding.	Run control scripts are not more permissive than 755.			

UNIX-LINUX-59	AC-3, AC-5, AC-6	Checks to see if run control scripts have the sgid or suid bit set.	Check run control scripts for sgid and suid: − Solaris # cd /etc # ls –lL rc* # cd /etc/init.d # ls –l − HP-UX # cd /sbin # ls –lL rc* # cd /sbin/init.d # ls –l # /etc/rc.config.d # ls -l − AIX # cd /etc # ls –lL rc* − Linux # cd /etc (may vary) # ls –lL rc* # cd /etc/init.d # ls –l If run control scripts have the sgid or suid bit set, then this is a finding.	Run control scripts do not have the sgid or the suid bit set.			
UNIX-LINUX-60	AC-3, AC-6	Checks to see if run control scripts execute world writeable programs or scripts.	Perform more command to look in the system startup files to check for files or scripts being executed. Check the permissions on the files or scripts to check if they are world writable. Alternatively, the command # find / -perm –0002 –type f > wwlist Will give a list of world writable files that can be checked against the executed files or scripts. If world writeable files are found to be executed from systems startup scripts, then this is a finding.	Run control scripts execute world writable programs or scripts.			

UNIX-LINUX-61	AC-3,	Checks to see if run control scripts are not owned by root or bin.	Check run control scripts ownership: − Solaris # cd /etc # ls –lL rc* # cd /etc/init.d # ls –l − HP-UX # cd /sbin # ls –lL rc* # cd /sbin/init.d # ls –l # /etc/rc.config.d # ls -l − AIX # cd /etc # ls –lL rc* − Linux # cd /etc (may vary) # ls –lL rc* # cd /etc/init.d # ls –l If run control scripts are not owned by root or bin, then this is a finding.	Run control scripts are owned by root or bin.			

UNIX-LINUX-62	AC-3.	Checks to see if run control scripts are not group owned by root, sys, bin, other or the system default.	Check run control scripts group ownership: − Solaris # cd /etc # ls –lL rc* # cd /etc/init.d # ls –lL − HP-UX # cd /sbin # ls –lL rc* # cd /sbin/init.d # ls –lL − AIX # cd /etc # ls –lL rc* − Linux # cd /etc (may vary) # ls –lL rc* # cd /etc/init.d # ls –lL rc* If run control scripts are not group owned by root, sys, bin, other or the system default, then this is a finding.	Run control scripts are group owned by root, sys, bin, other, or the system default.			
UNIX-LINUX-63	AC-3, AC-6	Checks to see if global initialization files are more permissive than 644.	Check global initialization files permissions: # ls –l /etc/.login # ls –l /etc/profile # ls –l /etc/bashrc # ls –l /etc/environment # ls –l /etc/security/environ If global initialization files are more permissive than 644, then this is a finding.	Global initialization files are not more permissive than 644.			

UNIX-LINUX-64	AC-3, AC-6	Checks to see if global initialization files are owned by root.	Check global initialization files ownership: # ls –l /etc/.login # ls –l /etc/profile # ls –l /etc/bashrc # ls –l /etc/environment # ls –l /etc/security/environ If global initialization files are not owned by root, then this is a finding.	Global initialization files are owned by root.			
UNIX-LINUX-65	AC-3, AC-6	Checks to see if global initialization files are group owned by root, sys,bin, other or the system default.	Check global initialization files group ownership: # ls –l /etc/.login # ls –l /etc/profile # ls –l /etc/bashrc # ls –l /etc/environment # ls –l /etc/security/environ If global initialization files are not group owned by root, sys, bin, other, or the system default, then this is a finding.	Global initialization files are group owned by root, sys, bin, other, or the system default.			
UNIX-LINUX-66	AC-3, AC-6	Checks to see if the default skeleton dot file permissions are more permissive than 644.	Check skeleton files permissions: − AIX. # ls –l /etc/security/.profile − All Other Platforms # ls –alL /etc/skel If skeleton dot files are more permissive than 644, then this is a finding.	Default skeleton . files are not more permissive than 644.			

UNIX-LINUX-67	AC-3, AC-6	Checks to see if default skeleton dot files are owned by root or bin.	Check skeleton files ownership: − AIX. # ls –l /etc/security/.profile − All Other Platforms # ls –alL /etc/skel If skeleton dot files are not owned by root or bin, then this is a finding.	Default skeleton . files are owned by root or bin.			
UNIX-LINUX-68	AC-3, AC-6	Checks to see if local initialization files are not owned by the user or root.	# ls –al /<usershomedirectory>/.login # ls –al /<usershomedirectory>/.cschrc # ls –al /<usershomedirectory>/.logout # ls –al /<usershomedirectory>/.profile # ls –al /<usershomedirectory>/.bash_profile # ls –al /<usershomedirectory>/.bashrc # ls –al /<usershomedirectory>/.bash_logout # ls –al /<usershomedirectory>/.env # ls –al /<usershomedirectory>/.dtprofile # ls –al /<usershomedirectory>/.dispatch # ls –al /<usershomedirectory>/.emacs # ls –al /<usershomedirectory>/.exrc If local initialization files are not owned the home directory user, then this is a finding. Local initialization files not owned by the user must be justified and documented by the ISSO	Local initialization files are owned by the user or root.			

UNIX-LINUX-69	AC-3, AC-6	Checks to see if the local initialization files are more permissive than 740.	# ls –al /<usershomedirectory>/.login # ls –al /<usershomedirectory>/.cschrc # ls –al /<usershomedirectory>/.logout # ls –al /<usershomedirectory>/.profile # ls –al /<usershomedirectory>/.bash_profile # ls –al /<usershomedirectory>/.bashrc # ls –al /<usershomedirectory>/.bash_logout # ls –al /<usershomedirectory>/.env # ls –al /<usershomedirectory>/.dtprofile (permissions should be 755) # ls –al /<usershomedirectory>/.dispatch # ls –al /<usershomedirectory>/.emacs # ls –al /<usershomedirectory>/.exrc If local initialization files are more permissive than 740 or the .dtprofile file is more permissive than 755, then this is a finding.	Local initialization files are not more permissive than 740. - .dt (a directory, this should have permissions of 755) - .dtprofile (a file, this should have permissions of 755)			
UNIX-LINUX-70	AC-3, AC-6	Checks to see if local initialization have the sgid or suid bit set.	# ls -la /<usershomedirectory>/.* If any of the above files have the suid or sgid bit set, then this is a finding.	Local initialization files do not have the suid or the sgid bit set.			
UNIX-LINUX-71	AC-3, AC-6	Checks the to see if the local files initialization execute world writeable programs or scripts.	# more /<usershomedirectory>/.* Look for programs or scripts executed within the local initialization files, and issue an ls -al on any programs or scripts found to check if the called program or script is world writable. If local initialization files execute world writable programs or scripts, then this is a finding.	Local initialization files do not execute world writable programs or scripts.			
UNIX-LINUX-72	AC-3, IA-2, IA-4	Checks to see if the.netrc file exists.	# find / -name .netrc If the .netrc file exists, then this is a finding. The .netrc must be justified and documented with the ISSO.	A .netrc file does not exist.			

UNIX-LINUX-73	AC-3, IA-2, IA-3, IA-4	.rhosts, .shosts, or hosts.equiv files contain other than hosts-user pairs.	# find / -name .rhosts # more /<directorylocation>/.rhosts # find / -name .shosts # more /<directorylocation>/.shosts # find / -name hosts.equiv # more /<directorylocation>/hosts.equiv # find / -name shosts.equiv # more /<directorylocation>/shosts.equiv If the .rhosts, .shosts, hosts.equiv, or shosts.equiv files contain other than hostname-user pairs and are not justified and documented with the ISSO, then this is a finding.	The .rhosts, .shosts, hosts.equiv, or shosts.equiv files do not contain other than host-user pairs and are not justified and documented with the ISSO.			
UNIX-LINUX-74	AC-3, IA-2, IA-4	Checks to see if the .rhosts, .shosts, hosts.equiv or shosts.equiv are used.	# find / -name .rhosts # find / -name .shosts # find / -name hosts.equiv # find / -name shosts.equiv If .rhosts, .shosts, hosts.equiv, or shosts.equiv are found and not justified and documented with the ISSO, then this is a finding.	The .rhosts, .shosts, hosts.equiv, or shosts.equiv are not used or are justified and documented with the ISSO.			

UNIX-LINUX-75	AC-3, AC-6	Checks to see if shell files have the suid bit set.	− AIX. # more /etc/security/login.cfg For each shell listed in the /etc/security/login.cfg file: # ls –l <shell> − All Other Platforms # find / -name “*sh” For each shell found: # ls –l <shell> If shell files have the suid bit set, then this is a finding. Note: The remsh command is sometimes linked to the rsh command and will have the suid bit set; in this case it is not a finding. Determine if that is the case by using ls –li to determine if they share the same inode number. The remsh command is the remote shell command and should not be considered a shell. Solaris uses the /usr/bin/rsh and the /usr/ucb/rsh commands for remote shells, and they should also be ignored here. A restricted shell also exists for bash (rbash).	Shell files do not have the suid bit set.			
UNIX-LINUX-76	AC-3, AC-6	Checks to see if shell files have the sgid bit set.	− AIX. # more /etc/security/login.cfg For each shell listed in the /etc/security/login.cfg file: # ls –l <shell> − All Other Platforms # find / -name “*sh” For each shell found: # ls –l <shell> If shell files have the sgid bit set, then this is a finding.	Shell files do not have the sgid bit set.			

UNIX-LINUX-77	AC-3, AC-6	Checks to see if shell files exist that are not owned by root or bin.	− AIX. # more /etc/security/login.cfg For each shell listed in the /etc/security/login.cfg file: # ls –l <shell> − All Other Platforms # find / -name “*sh” For each shell found: # ls –l <shell> If shell files are not owned by root or bin, then this is a finding.	Shell files are owned by root or bin.			
UNIX-LINUX-78	AC-3, AC-6	Checks to see if shell files permissions are more permissive than 755.	− AIX. # more /etc/security/login.cfg For each shell listed in the /etc/security/login.cfg file: # ls –l <shell> − All Other Platforms # find / -name “*sh” For each shell found: # ls –l <shell> If shell files are more permissive than 755, then this is a finding.	Shell files are not more permissive than 755.			
UNIX-LINUX-79	AC-3, AC-6	Checks to see if device file directories are writeable by users other than a system account or as configured by the vendor.	# ls –al /dev # ls –al /devices (Solaris) Check the permissions on the directories and subdirectories that contain device files. If device file directories are writable by users other than a system account or as configured by the vendor, then this is a finding.	Device file directories are not writable by users other than a system account or as configured by the vendor.			
UNIX-LINUX-80	AC-3, AC-6,	Checks to see if device files used for backup are readable and/or writeable by users other than root or a pseudo backup user.	Attempt to determine if any backup devices exist for the system. Some systems will have a file containing the default device files (such as /etc/default/tar on Solaris). Others can be checked via a system administration GUI (such as SAM on HP-UX). If backup device files exists and is readable or writeable by a user other than root or a pseudo backup user, ask the SA or if the file(s) are documented with the ISSO	Device files used for backup are writable by users other than root or a pseudo backup user.			

UNIX-LINUX-81	AC-3, AC-6	Checks to see if an audio device is more permissive than 644.	- SOLARIS # ls –lL /dev/audio - HP-UX # /usr/sbin/ioscan –f # ls –lL <audio device file> - AIX # /usr/sbin/lsdev –C | grep –I audio # ls –lL /dev/*aud0 - IRIX # ls –lL /dev/audio - Linux # ls -lL /dev/audio* If the permissions are greater than 644, then this is a finding.	An audio device is not more permissive than 644.			
UNIX-LINUX-82	AC-3, AC-6	Checks to see if an audio device is not owned by root.	- SOLARIS # ls –lL /dev/audio - HP-UX # /usr/sbin/ioscan –f # ls –lL <audio device file> - AIX # /usr/sbin/lsdev –C | grep –I audio # ls –lL /dev/*aud0 - IRIX # ls –lL /dev/audio - Linux # ls -lL /dev/audio* If the audio device is not owned by root, then this is a finding.	An audio device is owned by root.			

UNIX-LINUX-83	AC-3, AC-6	Checks to see if an audio device is not group owned by root, sys, or bin.	- SOLARIS # ls –lL /dev/audio - HP-UX # /usr/sbin/ioscan –f # ls –lL <audio device file> - AIX # /usr/sbin/lsdev –C | grep –I audio # ls –lL /dev/*aud0 - IRIX # ls –lL /dev/audio - Linux # ls -lL /dev/audio* If the audio device group ownership is not root, sys, bin, or audio, then this is a finding.	An audio device is group owned by root, sys, or bin.			
UNIX-LINUX-84	AC-3, AC-6	Checks for the ownership permissions and location of files with the suid bit set.	# find / perm –4000 | more If the ownership, permissions, and location of files with the suid bit set are not baselined with the ISSO, then this is a finding.	The ownership, permissions, and location of files with the suid bit set are documented with the ISSO.			
UNIX-LINUX-85	AC-3,	Checks for SUID files; checks to see if this process is performed weekly against the baseline.	find / perm –4000 |more Ask the SA If the system is checked weekly against the system baseline for unauthorized suid files as well as unauthorized modification to authorized suid files, if not then this is a finding.	The system is checked weekly against the system baseline for unauthorized suid files as well as unauthorized modification to authorized suid files.			
UNIX-LINUX-86	AC-3, AC-6	Checks to see if user file systems, removable media, or remote file systems are not mounted with the nosuid option invoked.	mount | grep –v nosuid Confirm all NFS mounts, floppy & CD drives, and user file systems (e.g., /export/home or /usr/home) are configured with the nosuid option. If user file systems, removable media, or remote file systems that do not require suid/sgid files are not mounted with the nosuid option invoked, then this is a finding.	User file systems, removable media, or remote file systems are mounted with the nosuid option invoked.			

UNIX-LINUX-87	AC-3, AC-6	Checks the ownership permissions and location of files with the suid bit; checks to see if they are documented with the ISSO.	# find / perm –2000 |more If the ownership, permissions, and location of files with the sgid bit set are not baselined with the ISSO, then this is a finding.	The ownership, permissions, and location of files with the sgid bit set are documented with the ISSO			
UNIX-LINUX-88	AC-3, AC-6,	Checks for the existance of SGID files; checks to see if they are checked weekly against the baseline.	find / perm –2000 |more If the system is not checked weekly against the system baseline for unauthorized sgid files as well as unauthorized modification to authorized sgid files, then this is a finding.	The system is checked weekly against the system baseline for unauthorized sgid files as well as unauthorized modification to authorized sgid files.			
UNIX-LINUX-89	AC-14, AC-17, SC-2	Checks to see if services that allow interaction without authentication or via anonymous authentication are documented, justified to the ISSO, and are properly secured and segregated from other systems that contain services that explicitly require authentication and identity verification.	Determine if the organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives. Examples are access to public facing government service websites such as www.firstgov.gov.	Services that allow interaction without authentication or via anonymous authentication are documented, justified to the ISSO, and are properly secured and segregated from other systems that contain services that explicitly require authentication and identity verification.			
UNIX-LINUX-90	AC-3, AC-6	Checks to see if there are world writeable files or directories that have not been determined to be public directories.	# find / -type f -perm -002 |more If there are world writable files, then this is a finding. # find / -type d -perm -002 |more If there are world writable directories that are not public directories (e.g., /tmp), then this is a finding.	There are no world writable files or world writable directories other than those determined to be public files or directories.			
UNIX-LINUX-91	AC-3, AC-6	Checks to see if public directories are not owned by root, or an application user.	find / -type d \(-perm -002 -a –perm –1000 \) |more If public directories are not owned by root or an application user, then this is a finding.	Public directories are owned by root or an application user.			

UNIX-LINUX-92	AC-3, AC-6	Checks to see if public directories are not group owned by root, sys, bin, or an application group.	ls –ld `find / -type d \( -perm -002 -a –perm –1000 \)` |more If public directories are not group owned by root, sys, bin, other or an application group, then this is a finding.	Public directories are group owned by root, sys, bin, or an application group.			
UNIX-LINUX-93	AC-3, AC-6	The system and user default umask is not 027.	− AIX # /usr/sbin/lsuser –a umask ALL | more − All other platforms - Global Initialization Files # grep umask /etc/* Confirm the global initialization files set the umask to 027. - Local Initialization Files # grep umask /<usershomedirectory>/.* Confirm the local initialization files do not exceed the default umask to 027. Note: If the default umask is 000 or allows for the creation of world writable files this becomes a Severity Code I finding. If the system and user default umask is not 027, then this a finding.	The system and user default umask is 027.			
UNIX-LINUX-94	AC-2, AC-3, IA-2, IA-4	Check to see if unused default accounts have been disabled.	To determine if unused default system accounts such as those for sys, bin, uucp, nuucp, daemon, smtp, etc., have been disabled perform the following: − Solaris # grep “*LK*” /etc/shadow − HP-UX # grep u_lock /tcb/files/auth/b/bin Repeat for other system accounts. − AIX # grep account_locked /etc/security/user − Linux # awk –F: ‘$2 == “*” {print $0}’ /etc/shadow If there are any unused default system accounts that are not locked or have false for a shell, then this is a finding.	Unused default accounts have been disabled.			

UNIX-LINUX-95	AC-3, AU-6, AC-13	Checks to see if auditing is implemented.	Perform the following to determine if auditing is enabled: − Solaris # ps –ef |grep auditd − HP-UX # audsys − AIX # /usr/sbin/audit query | head -1 − Linux # ps –ef |grep auditd If the auditd process is not found, then this is a finding.	Auditing is implemented.			
UNIX-LINUX-96	AC-3, AC-6, AU-9	System audit logs are readable by unauthorized users.	Perform the following to determine the location of audit logs and then check the ownership: − Solaris # more /etc/security/audit_control # ls –lLd <audit log dir> − HP-UX # ls –la /.secure/etc/* − AIX # grep ":bin:" /etc/security/audit/config Directories to search will be listed under the bin stanza. # ls –la <audit directories> − Linux # ls –la /var/log/audit.d # ls –la /var/log/audit/audit.log If any of the audit log files are readable by unprivileged id's, then this is a finding.	System audit logs are not readable by unauthorized users.			

UNIX-LINUX-97	AC-3, AC-6, AU-9	Checks to see if system audit logs are more permissive than 640.	Perform the following to determine the location of audit logs and then check the permissions: − Solaris # more /etc/security/audit_control # ls –la <audit log dir> − HP-UX # ls –la /.secure/etc − AIX # grep ":bin:" /etc/security/audit/config Directories to search will be listed under the bin stanza. # ls –la <audit directories> − Linux # ls –la /var/log/audit.d # ls –la /var/log/audit/audit.log If any of the audit log file permissions are greater than 640, then this is a finding.	System audit logs are not more permissive than 640.			
UNIX-LINUX-98	AC-3, AU-3	Checks to see if the audit system is configured to audit failed attempts to access files and programs.	− Solaris # more /etc/security/audit_control Confirm flags –fr or fr is configured. − HP-UX # grep –i "audevent_args1" /etc/rc.config.d/auditing \ | grep open − AIX # more /etc/security/audit/events Confirm the following events are configured: FILE_Open − Linux For LAUS: # grep "@open-ops" /etc/audit/filter.conf For auditd: # grep "-a exit,always –S open –F success!=0" /etc/audit.rules (RHEL5 /etc/audit/audit.rules)	The audit system is configured to audit failed attempts to access files and programs.			

UNIX-LINUX-99	AC-3, AU-3	Checks to see if the audit system is configured to audit files and programs deleted by the user.	− Solaris # grep flags /etc/security/audit_control Confirm flags fd or +fd and -fd is configured. − HP-UX # grep –i “audevent_args1” /etc/rc.config.d/auditing \ | grep delete − AIX # more /etc/security/audit/events Confirm the following events are configured: FILE_Unlink, FS_Rmdir − Linux For LAUS: # grep “@rmdir-ops” /etc/audit/filter.conf # grep “@unlink-ops” /etc/audit/filter.conf For auditd: # grep “-a exit,always –S unlink –S rmdir” /etc/audit.rules (RHEL5 /etc/audit/audit.rules)	The audit system is configured to audit files and programs deleted by the user.			

UNIX-LINUX-100	AC-2, AC-3, AU-3	Checks to see if the audit system is configured to audit all administrative, privileged and security actions.	− Solaris 2.5 through 9
			# grep flags /etc/security/audit_control
			Confirm flags ad or +ad and -ad is configured.
			− Solaris 10 and some prior versions of 8 and 9
			# grep flags /etc/security/audit_control
			Confirm am or +am and -am is configured.
			− HP-UX
			# grep –i “audevent_args1” /etc/rc.config.d/auditing \
			  | grep admin
			# grep –i “audevent_args1” /etc/rc.config.d/auditing \
			  | grep removable
			− AIX # more /etc/security/audit/events
			Confirm the following events are configured:
			ACCT_Disable, ACCT_Enable, AUD_it, BACKUP_Export, DEV_Change, DEV_Configure, DEV_Create, FILE_Chpriv, FILE_Fchpriv, FILE_Mknod, FILE_Owner, FS_Chroot, FS_Mount, FS_Umount, PASSWORD_Check, PROC_Adjtime,PROC_Kill, PROC_Privilege, PROC_Setpgid, PROC_SetUserIds, RESTORE_Import, TCBCK_Delete, USER_Change, USER_Create, USER_Reboot, USER_Remove, and USER_SetEnv
			− Linux For LAUS: # grep “@priv-ops” /etc/audit/filter.conf
			  # grep “@mount-ops” /etc/audit/filter.conf
			  # grep “@system-ops” /etc/audit/filter.conf
			  For auditd the following should be present in /etc/audit.rules: (RHEL5 /etc/audit/audit.rules)
			  -w /etc/auditd.conf
			  -w /etc/audit.rules
			  -a exit,always –S stime –S acct –S reboot –S swapon
			  -a exit,always –S settimeofday –S setrlimit –S setdomainname
			  -a exit,always –S sched_setparam –S sched_setscheduler
				The audit system is configured to audit all administrative, privileged, and security actions.			

UNIX-LINUX-101	AC-2, AC-3, AU-3	Checks to see if the audit system is configured to audit login, logout and session initiation.	− Solaris # egrep “flags|naflags” /etc/security/audit_control Confirm flags lo or +lo and -lo is configured. Confirm naflags lo or +lo and –lo is configured. − HP-UX # grep –i “audevent_args1” /etc/rc.config.d/auditing \ | grep login − AIX # more /etc/security/audit/events Confirm the following events are configured: USER_Login, USER_Logout, INIT_Start, INIT_End and USER_SU − Linux For LAUS: # grep process-login /etc/audit/filter.conf |grep always For auditd: This is not a finding. Auditd enables this by default in the source code.	The audit system is configured to audit login, logout, and session initiation.			

UNIX-LINUX-102	AC-3, AU-9	Checks to see if the audit system is configured to audit all discretionary access control permission modifications.	− Solaris # grep flags /etc/security/audit_control Confirm flags fm or +fm and -fm is configured. − HP-UX # grep –i “audevent_args1” /etc/rc.config.d/auditing \ # | grep moddac − AIX # more /etc/security/audit/events Confirm the following events are configured: FILE_Acl, FILE_Fchmod, FILE_Fchown, FILE_Mode and FILE_Owner − Linux For LAUS: # grep “@mode-ops” /etc/audit/filter.conf # grep “@owner-ops” /etc/audit/filter.conf (RHEL5 /etc/audit/audit.rules) For auditd the following system calls should be present in /etc/audit.rules: -a exit,always –S chmod –S fchmod –S chown –S chown32 –S fchown -a exit,always –S fchown32 –S lchown –S lchown32 (RHEL5 /etc/audit/audit.rules)	The audit system is configured to audit all discretionary access control permission modifications.			
UNIX-LINUX-103	AU-9	Checks to see if audit logs are rotated daily.	Perform the following to search the crontab for entries to rotate the audit logs. # crontab –l # less /etc/logrotate.conf can be checked for daily logrotation as well If a program can be located, this is not a finding. Otherwise, query the SA. If there is one that is demonstrable (and runs automatically), this is not a finding. If the SA runs it manually, it is still a finding, because if the SA is not there, it will not be accomplished. If the audit output is not archived daily, to tape or disk, this is a finding. This can be ascertained by looking at the audit log directory and, if more than one file is there, or if the file does not have today’s date, this is a finding.	Audit logs are rotated daily.			

UNIX-LINUX-104	AC-13, AU-6	Checks to see if audit trails and/or system logs are reviewed on a daily basis(or an interval stated in local policy).	Ask the SA/ISSO if audit files are reviewed daily (or as stated by a policy interval) If the audit files are not reviewed daily (or according to local policy), then this is a finding.	Audit trails and/or system logs are reviewed on a daily basis for: - Excessive logon attempt failures by single or multiple users - Logons at unusual/non-duty hours - Failed attempts to access restricted system or data files indicating a possible pattern of deliberate browsing - Unusual or unauthorized activity by System Administrators - Command-line activity by a user that should not have that capability - System failures or errors - Unusual or suspicious patterns of activity			
UNIX-LINUX-105	AC-3	Checks to see if access to the cron utility is controlled via the cron.allow and/or cron.deny files.	Verify the cron.allow and cron.deny files exist: − Solaris # ls –lL /etc/cron.d/cron.allow # ls –lL /etc/cron.d/cron.deny − HP-UX # ls –lL /var/adm/cron/cron.allow # ls –lL /var/adm/cron/cron.deny − AIX # ls –lL /var/adm/cron/cron.allow # ls –lL /var/adm/cron/cron.deny − Linux Red Hat # ls –lL /etc/cron.allow # ls –lL /etc/cron.deny Or SuSE # ls –lL /var/spool/cron/allow # ls –lL /var/spool/cron/deny If the cron.allow or cron.deny files do not exist, then this is a finding.	Access to the cron utility is controlled via the cron.allow and/or cron.deny file(s).			

UNIX-LINUX-106	AC-3, AC-5, AC-6	Checks to see if the cron.allow file is more permissive than 600.	− Solaris # ls –lL /etc/cron.d/cron.allow − HP-UX # ls –lL /var/adm/cron/cron.allow − AIX # ls –lL /var/adm/cron/cron.allow − Linux Red Hat # ls –lL /etc/cron.allow Or SuSE # ls –lL /var/spool/cron/allow If the cron.allow file is more permissive than 600, then this is a finding.	The cron.allow file is not more permissive than 600.			
UNIX-LINUX-107	AC-3	Checks to see if default system accounts with the exception of root are listed in the cron.allow file or excluded from the cron.deny file if cron.allow does not exist.	Check for default system accounts in the following: − Solaris # more /etc/cron.d/cron.allow − HP-UX # more /var/adm/cron/cron.allow − AIX # more /var/adm/cron/cron.allow − Linux Red Hat # more /etc/cron.allow Or SuSE # more /var/spool/cron/allow Default accounts (such as bin, sys, adm, and others) will not be listed in the cron.allow file or this will be a finding.	Default system accounts (with the possible exception of root) are not listed in the cron.allow file or excluded from the cron.deny file if cron.allow does not exist.			

UNIX-LINUX-108	AC-3, AC-6	Checks to see if crontab files are more permissive than 600. 700 on some linux systems.	− Solaris # ls –lL /var/spool/cron/crontabs/ − HP-UX # ls –lL /var/spool/cron/crontabs/ − AIX # ls –lL /var/spool/cron/crontabs/ − Linux # ls –lL /var/spool/cron/ (Permissions of 600) # ls –lL /etc/cron.d/ (Permissions of 600) # ls –lL /etc/crontab (Permissions of 600) # ls –lL /etc/cron.daily/ (Permissions of 700) # ls –lL /etc/cron.hourly/ (Permissions of 700) # ls –lL /etc/cron.monthly/ (Permissions of 700) # ls –lL /etc/cron.weekly/ (Permissions of 700) If crontab files are more permissive than 600 (700 for some Linux files), then this is a finding.	Crontab files are not more permissive than 600 (700 for some Linux files).			
UNIX-LINUX-109	AC-3, AC-6	Checks to see if the cron or crontab directories are more permissive than 755.	− Solaris # ls –ld /var/spool/cron/crontabs − HP-UX # ls –ld /var/spool/cron/crontabs − AIX # ls –ld /var/spool/cron/crontabs − Linux # ls –ld /var/spool/cron # ls –ld /etc/cron.d # ls –ld /etc/cron.daily # ls –ld /etc/cron.hourly # ls –ld /etc/cron.monthly # ls –ld /etc/cron.weekly If the cron or crontab directories are more permissive than 755, then this is a finding.	The cron or crontab directories are not more permissive than 755.			

UNIX-LINUX-110	AC-3, AC-6	Checks to see if the cron or crontab directories are owned by root or bin.	− Solaris # ls –ld /var/spool/cron/crontabs − HP-UX # ls –ld /var/spool/cron/crontabs − AIX # ls –ld /var/spool/cron/crontabs − Linux # ls –ld /var/spool/cron # ls –ld /etc/cron.d # ls –ld /etc/cron.daily # ls –ld /etc/cron.hourly # ls –ld /etc/cron.monthly # ls –ld /etc/cron.weekly If the cron or crontab directories are not owned by root or bin, then this is a finding.	The cron or crontab directories are owned by root or bin.			
UNIX-LINUX-111	AC-3, AC-6	Checks to see if the cron or crontab directories are group owned by root, sys, or bin.	− Solaris # ls –ld /var/spool/cron/crontabs − HP-UX # ls –ld /var/spool/cron/crontabs − AIX # ls –ld /var/spool/cron/crontabs − Linux # ls –ld /var/spool/cron # ls –ld /etc/cron.d # ls –ld /etc/cron.daily # ls –ld /etc/cron.hourly # ls –ld /etc/cron.monthly # ls –ld /etc/cron.weekly If the cron or crontab directories are not group owned by root, sys, or bin, then this is a finding.	The cron or crontab directories are not group owned by root, sys, or bin.			

UNIX-LINUX-112	AC-13, AU-6,	Checks to see if cron logging is implemented.	− Solaris
			# ls –lL /var/cron/log
			# more /etc/default/cron
			CRONLOG=YES
			If this line does not exist, this is a finding.
			
			− HP-UX
			# ls –lL /var/adm/cron/log
			Cron is logged by default.
			
			− AIX
			# ls –lL /var/adm/cron/log
			Cron is logged by default.
			
			− IRIX
			# ls –lL /var/cron/log
			
			− Linux
			Cron logging is controlled by the syslog on Linux:
			
			# grep cron* /etc/syslog.conf
			
			Red Hat
			# ls –lL /var/log/cron
			
			SuSE
			# ls –lL /var/log/messages
			
			If an entry for cron is not found, then this is a finding.
				Cron logging is implemented.			

UNIX-LINUX-113	AC-3, AC-6	Checks to see if the cron log file is more permissive than 600.	− Solaris # ls –lL /var/cron/log − HP-UX # ls –lL /var/adm/cron/log − AIX # ls –lL /var/adm/cron/log − Linux Red Hat # ls –lL /var/log/cron SuSE # ls –lL /var/log/messages If the cronlog file is more permissive than 600, then this is a finding.	The cronlog file is not more permissive than 600.			
UNIX-LINUX-114	AC-3, AC-6	Checks to see if the cron.deny is more permissive than 600.	− Solaris # ls –lL /etc/cron.d/cron.deny − HP-UX # ls –lL /var/adm/cron/cron.deny − AIX # ls –lL /var/adm/cron/cron.deny − IRIX # ls –lL /etc/cron.d/cron.deny − Linux Red Hat # ls –lL /etc/cron.deny Or SuSE # ls –lL /var/spool/cron/deny If the cron.deny file is more permissive than 600, then this is a finding.	The cron.deny file is not more permissive than 600.			

UNIX-LINUX-115	AC-3, AC-6,	Checks to see if the cron.allow file is owned and group owned by root.	− Solaris # ls –lL /etc/cron.d/cron.allow − HP-UX # ls –lL /var/adm/cron/cron.allow − AIX # ls –lL /var/adm/cron/cron.allow − Linux Red Hat # ls –lL /etc/cron.allow Or SuSE # ls –lL /var/spool/cron/allow If the cron.allow file is not owned and group owned by root, sys, or bin, then this is a finding.	The cron.allow file is owned and group owned by root, sys or bin.			
UNIX-LINUX-116	AC-3, AC-6,	Checks to see if the cron.deny file is owned and group owned by root.	− Solaris # ls –lL /etc/cron.d/cron.deny − HP-UX # ls –lL /var/adm/cron/cron.deny − AIX # ls –lL /var/adm/cron/cron.deny − Linux Red Hat # ls –lL /etc/cron.deny Or SuSE # ls –lL /var/spool/cron/deny If the cron.deny file is not owned and group owned by root, sys, or bin, then this is a finding.	The cron.deny file is owned and group owned by root, sys, or bin.			

UNIX-LINUX-117	AC-3, AC-6	Checks to see if access to the at utility is controlled via the at.allow and at.deny files.	Verify the at.allow and/or at.deny files exist. − Solaris # ls –lL /etc/cron.d/at.allow # ls –lL /etc/cron.d/at.deny − HP-UX # ls –lL /var/adm/cron/at.allow # ls –lL /var/adm/cron/at.deny − AIX # ls –lL /var/adm/cron/at.allow # ls –lL /var/adm/cron/at.deny − Linux # ls –lL /etc/at.allow # ls –lL /etc/at.deny Ensure at least one of the above files exists.	Access to the at utility is controlled via the at.allow and/or at.deny file(s).			
UNIX-LINUX-118	AC-3, AC-6	Checks to see if the at.deny file exists and is empty.	− Solaris # more /etc/cron.d/at.deny − HP-UX # more /var/adm/cron/at.deny − AIX # more /var/adm/cron/at.deny − Linux # more /etc/at.deny If the at.deny file exists and is empty, then this is a finding.	The at.deny file does not exist. OR The at.deny file exists and is not empty.			

UNIX-LINUX-119	AC-3, AC-6	Checks to see if default accounts are listed in the at.allow file.	− Solaris # more /etc/cron.d/at.allow − HP-UX # more /var/adm/cron/at.allow − AIX # more /var/adm/cron/at.allow − Linux # more /etc/at.allow Default accounts (such as bin, sys, adm, and others) will not be listed in the at.allow file or this will be a finding.	Default system accounts (with the exception of root) are not listed in the at.allow file or not excluded from the at.deny file if at.allow does not exist.			
UNIX-LINUX-120	AC-3, AC-5, AC-6	Checks to see if the at.allow or at.deny file is more permissive than 600.	− Solaris # ls –lL /etc/cron.d/at.allow # ls –lL /etc/cron.d/at.deny − HP-UX # ls –lL /var/adm/cron/at.allow # ls –lL /var/adm/cron/at.deny − AIX # ls –lL /var/adm/cron/at.allow # ls –lL /var/adm/cron/at.deny − IRIX # ls –lL /etc/cron.d/at.allow # ls –lL /etc/cron.d/at.deny − Linux # ls –lL /etc/at.allow # ls –lL /etc/at.deny If the at.allow or at.deny file(s) is more permissive than 600, then this is a finding.	The at.allow or at.deny file(s) is not more permissive than 600.			

UNIX-LINUX-121	AC-3, AC-6	Checks to see if the at or equivalent directory is more permissive than 755.	Check the permissions of the at directory by performing the following: # ls –ld /var/spool/cron/atjobs Or # ls –ld /var/spool/atjobs If the directory permissions are greater than 755, then this is a finding.	The at (or equivalent) directory is not more permissive than 755.			
UNIX-LINUX-122	AC-3, AC-6,	Checks to see if the at directory is owned by root, bin, sys, or daemon.	Check the ownership of the at directory by performing the following: # ls –ld /var/spool/cron/atjobs Or # ls –ld /var/spool/atjobs If the directory is not owned by root, sys, bin, or daemon, then this is a finding.	The at directory is owned by root, sys, bin, or daemon.			
UNIX-LINUX-123	AC-3, AC-6,	At programs set the umask more permissive than 027 and these are not justified and documented with the ISSO.	Perform the following to check for at jobs: # cd /var/spool/cron/atjobs Or # cd /var/spool/atjobs Determine if there are any at jobs by viewing a long listing of the directory. If there are at jobs perform the following to check for any programs that may have a umask more permissive than 027: # grep umask ./* If there are any, this is a finding unless the ISSO has justifying documentation. If there are no ‘at’ jobs present, this vulnerability is Not Applicable.	At programs set the umask more permissive than 027 and these are justified and documented with the ISSO.			

UNIX-LINUX-124	AC-3, AC-6,	Checks to see if the at.allow file is owned and group owned by root.	− Solaris # ls –lL /etc/cron.d/at.allow − HP-UX # ls –lL /var/adm/cron/at.allow − AIX # ls –lL /var/adm/cron/at.allow − Linux # ls –lL /etc/at.allow If the at.allow file is not owned and group owned by root, sys, or bin, then this is a finding.	The at.allow file is owned and group owned by root, sys, or bin.			
UNIX-LINUX-125	AC-3, AC-6,	Checks to see if the at.deny file is owned and group owned by root, sys, or bin.	− Solaris # ls –lL /etc/cron.d/at.deny − HP-UX # ls –lL /var/adm/cron/at.deny − AIX # ls –lL /var/adm/cron/at.deny − Linux # ls –lL /etc/at.deny If the at.deny file is not owned and group owned by root, sys, or bin, then this is a finding.	The at.deny file is owned and group owned by root, sys, or bin.			
UNIX-LINUX-126	AC-3,AC-6	Checks to see if the inetd.conf or xinetd.conf file is owned by root or bin.	Check the permissions of inetd.conf file by: # ls –lL /etc/inetd.conf Or, for Linux systems # ls –lL /etc/xinetd.conf # ls –lL /etc/xinetd.d This is a finding if any of the above files or directories are not owned by root or bin.	The inetd.conf file (xinetd.conf file and the xinetd.d directory for Linux) is owned by root or bin.			

UNIX-LINUX-127	AC-3, AC-6	Checks to see if the inetd.conf file permissions are more permissive than 440. The linux xinetd.d is more permissive than 755.	Check the permissions of inetd.conf file by: # ls –lL /etc/inetd.conf Or, for Linux systems # ls –lL /etc/xinetd.conf # ls –lL /etc/xinetd.d This is a finding if permissions for the inetd.conf files are greater than 440. In addition, on Linux systems, the /etc/xinetd.d directory permissions should not be greater than 755.	The inetd.conf (xinetd.conf for Linux) file is not more permissive than 440. The Linux xinetd.d. directory is not more permissive than 755.			
UNIX-LINUX-128	AC-3, AC-6	Checks to see if the services file is owned by root or bin.	ls –lL /etc/services The services file is not owned by root or bin, then this is a finding	The services file is owned by root or bin.			
UNIX-LINUX-129	AC-3, AC-6	Checks to see if the services file is more permissive than 644.	ls –lL /etc/services If the services file is more permissive than 644, then this is a finding.	The services file is not more permissive than 644.			
UNIX-LINUX-130	AC-3,	Checks to see if remote login or remote shell is enabled.	Solaris, HP-UX, AIX, IRIX # grep –v "^#" /etc/inetd.conf |grep rlogind # grep –v "^#" /etc/inetd.conf |grep rshd Solaris 10 # svcs rlogin Linux # grep disable /etc/xinetd.d/rlogin # grep disable /etc/xinetd.d/rsh If either rlogin or rsh are found to be enabled, then this is a finding.	Remote login or remote shell is disabled			

UNIX-LINUX-131	AC-3,	Checks to see if the rexec service is enabled.	Perform the following to determine if the rexec service is enabled: Solaris, HP-UX, AIX, IRIX # grep –v “^#” /etc/inetd.conf |grep rexec Solaris 10 # svcs rexec |grep disabled Linux # grep disable /etc/xinetd.d/rexec If rexec is found to be enabled, then this is a finding.	The rexec service is disabled.			
UNIX-LINUX-132	AC-3,	Checks to see if network analysis tools are enabled.	Perform the following to determine if any network analysis tools are enabled: # find / -name ethereal # find / -name tcpdump # find / -name snoop (RHEL find / -name wireshark) If the any of the above network analysis tools are found, then this is a finding.	Network Analysis tools are disabled.			
UNIX-LINUX-133	AC-11	Checks to see if the system is a print server and the configuration is documented with the ISSO.	Ask the SA if the system is a print server or a client of another server. If it is either of these, ask the SA if it is documented with the ISSO. If the printer configuration is not documented with the ISSO, then this is a finding.	The system is a print server/client, and the configuration is documented with the ISSO.			

UNIX-LINUX-134	AC-3, AC-6	Checks to see if the hosts.lpd is owned by root, bin ,sys or lp.	Look for the presence of a print service configuration file by using the command: # find /etc –name hosts.lpd –print If this file does not exist, use the command: # find /etc –name Systems -print If this file does not exist, use the command: # find /etc –name printers.conf If neither of the files are found, then this check should be marked Not Applicable. Otherwise perform: # ls –lL <print service file> If the owner of the file is not root, sys, bin or lp, then this is a finding.	The hosts.lpd (or equivalent) file is owned by a root, sys, bin, or lp.			
UNIX-LINUX-135	AC-3, AC-5, AC-6	Checks to see if the permissions on the hosts.lpd file are more permissive than 664.	Look for the presence of a print service configuration file by using the command: # find /etc –name hosts.lpd –print If this file does not exist, use the command: # find /etc –name Systems -print If this file does not exist, use the command: # find /etc –name printers.conf If neither of the files are found, then this check should be marked Not Applicable. Otherwise perform: # ls –lL <print service file> and verify the permissions are not greater than 664. If the permissions are greater than 664, then this is a finding.	The hosts.lpd (or equivalent) file is more permissive than 664.			

UNIX-LINUX-136	AC-3, AC-6,	Checks to see if the traceroute command owner is root.	− Solaris # ls –lL /usr/sbin/traceroute − HP-UX # ls –lL /usr/sbin/traceroute − AIX # ls –lL /usr/bin/traceroute − Linux # ls –lL /usr/sbin/traceroute If the traceroute command is not owned by root, then this is a finding.	The traceroute command is owned by root.			
UNIX-LINUX-137	AC-3, AC-6,	Checks to see if the traceroute commands group owner is sys, bin, or root.	− Solaris # ls –lL /usr/sbin/traceroute − HP-UX # ls –lL /usr/sbin/traceroute − AIX # ls –lL /usr/bin/traceroute − Linux # ls –lL /usr/sbin/traceroute If the traceroute command is not group owned by root, sys, or bin, then this is a finding.	The traceroute command is group owned by root, sys, or bin.			
UNIX-LINUX-138	AC-3, AC-6	The traceroute command is more permissive than 700.	− Solaris # ls –lL /usr/sbin/traceroute − HP-UX # ls –lL /usr/sbin/traceroute − AIX # ls –lL /usr/bin/traceroute − Linux # ls –lL /usr/sbin/traceroute If the traceroute command is more permissive than 700, then this is a finding.	The traceroute command is not more permissive than 700.			

UNIX-LINUX-139	AC-3,	Checks to see if the browser/smart update feature is enabled.	This check will only apply to Netscape web browsers. All versions of Mozilla and Mozilla Firefox can check for new browser version, but will not automatically install them. Verify that automatic software installation is not enabled. Select Edit>>Preferences>>Advanced from the web browser toolbar. Drop down the Advanced submenu. The Advanced options submenu gives us the Software Installation settings. Verify the 'Enable software installation' setting is not checked. If it is checked, then this is a finding.	The browser SmartUpdate or software update feature is disabled.			
UNIX-LINUX-140	AC-3,	Checks to see if the browser has unencrypted secure content caching enabled.	This check is mainly pertaining to passwords or sensitive data that can be stored by the browser cache. Ensure the following setting is enabled: Edit>>Preferences>>Privacy&Security from the web browser toolbar. Select the Passwords sub-category and verify 'Use encryption when storing sensitive data' under the Encrypting versus Obscuring is checked. If it is not, then this is a finding. RHEL - FIREFOX - either set a master password for storing sensitive information or un-tick the box that allows the information to be stored.	The browser has unencrypted secure content caching disabled.			
UNIX-LINUX-141	AC-3	Checks to see if the browser issues a warning when form data is redirected.	To determine if a browser has browser data redirection warning enabled perform: Select Edit>>Preferences>Privacy and Security from the browser toolbar. Select the Validation (RHEL-FIREFOX-VERIFICATION) tab. Ensure that "Use OCSP to validate only certificates that specify an OCSP service URL" is selected under the OCSP heading. If it is not selected, then this is a finding.	The browser issues a warning when form data is redirected.			
UNIX-LINUX-142	AC-3	Checks to see if the browser homepage is configured for a blank page or a locally generated page.	Click on "Edit">>"Preferences">> "Navigator", and verify the "Blank Page" button under "Navigator Start With" is selected or, if Home Page is selected, verify the pathname under the Home Page box is for a local web server. For Firefox select Edit >> Preferences in the browser tool bar, and then select the General item.	The browser home page is a blank page or a locally generated page.			
UNIX-LINUX-143	AC-4,	Checks to see if the browser is configured for secure socket layer (SSLV2 and SSLv3).	To check if browsers are configured for SSL, select Edit >> Preferences in the browser tool bar, and then select the Privacy and Security menu item. Select the SSL tab and verify that "Enable SSL version 2" and "Enable SSL version 3" is checked under the SSL Protocol versions. If they are not, then this is a finding. (RHEL-FIREFOX Preferences-Advanced-Security)	The browser is configured for Secure Socket Layer (SSL) v2 and SSL v3.			
UNIX-LINUX-144	AC-3, AC-6, CA-2	Checks to see if the root account uses the browser for reasons other than to control local applications.	Look in the root account home directory for a .netscape or a .mozilla directory. If none exists, mark this check as Not A Finding. If there is one, verify with the root users and the ISSO what the intent of the browsing is. Some evidence may be obtained by using the browser to view cached pages under the .netscape directory.	The root account does not use the browser for reasons other than to control local applications.			

UNIX-LINUX-145	SI-2	Checks to see if the browser is not a supported version.	To view the version number click “Help” then click “About Browser” from the browser tool bar. If the browser version is not Netscape 4.79 or greater, or FireFox 1.5 or greater, then this is a finding.	The browser is a supported version.			
UNIX-LINUX-146	AC-3, AC-6	Checks to see if the alias file is owned by root.	Find the aliases file on the system: # find / -name aliases –depth –print # ls –lL <alias location> (NOTE: THE -depth OPTION may not be required. Tested on RHEL5) If the file is not owned by root, then this is a finding.	The aliases file is owned by root.			
UNIX-LINUX-147	AC-3, AC-6	Checks to see if the alias file is more permissive than 644.	Find the aliases file on the system: # find / -name aliases –depth –print # ls –lL <alias location> (NOTE: THE -depth OPTION may not be required. Tested on RHEL5) If the permissions are greater than 644, then this is a finding.	The aliases file is not more permissive than 644.			
UNIX-LINUX-148	AC-3, AC-6	Checks to see if files executed through an alias file are owned by root and reside within a directory owned and writeable only by root.	Find the aliases file on the system: # find / -name aliases –depth –print # more <aliases file location> (NOTE: THE -depth OPTION may not be required. Tested on RHEL5) Examine the aliases file for any directories or paths that may be utilized. Perform: # ls –lL <path> Ensure the file and parent directory are owned by root. If it is not, then this is a finding.	Files executed through an aliases file are owned by root and reside within a directory owned and writable only by root.			

UNIX-LINUX-149	AC-3, AC-6	Checks to see if files executed through an alias are more permissive than 755.	Find the aliases file on the system: # find / -name aliases –depth –print # more <aliases file location> (NOTE: THE -depth OPTION may not be required. Tested on RHEL5) Examine the aliases file for any directories or paths that may be utilized. Perform: # ls –lL <path> to check the permissions are not greater than 755. If files executed through an alias have permissions greater than 755, then this is a finding.	Files executed through an aliases file are not more permissive than 755.			
UNIX-LINUX-150	AU-2, AU-3, AU-8	Critical-level sendmail messages are not logged.	Enter the command: # more /etc/syslog.conf Ensure the configuration file logs mail.crit, mail.debug, mail.*, or *.crit. If the system is not logging critical sendmail messages, then this is a finding.	Critical-level sendmail messages are logged.			
UNIX-LINUX-151	AC-3, AC-6, AU-9	Checks to see if the critical sendmail logfile is owned by root.	Perform: # more /etc/syslog.conf Ensure the configuration file logs mail.crit, mail.debug, mail.*, or *.crit to a file. Perform: # ls -lL <file location> If the files is not owned by root, then this is a finding.	Critical sendmail log file is not owned by root.			

UNIX-LINUX-152	AC-3, AC-6	Checks to see if the critical sendmail logfile is more permissive than 644.	Perform: # more /etc/syslog.conf Ensure the configuration file logs mail.crit, mail.debug, mail.*, or *.crit to a file. Perform: # ls -lL <file location> If the log file permissions are greater than 644, then this is a finding.	Critical sendmail log file is not more permissive than 644.			
UNIX-LINUX-153	AC-3	Checks for the existance of .Forward files were found.	Search for any .forward files on the system by: # find –name .forward –print This is considered a finding if any .forward files are found on the system.	.forward files were not found.			
UNIX-LINUX-154	CM-7	Checks to see if an anonymous ftp server is active and not documented by the ISSO.	Perform the following to determine if a system is capable of anonymous ftp: # ps –ef |grep ftpd # grep ftp /etc/passwd Use the command ftp to activate the ftp service. Attempt to log into this host with a user name of anonymous and a password of guest (also try the password of guest@mail.com). If the logon is successful, ask if the use of anonymous FTP on the system is documented with the ISSO. If it is not, then this is a finding.	Anonymous FTP is not active or documented by the ISSO.			
UNIX-LINUX-155	IA-2, IA-4	Checks to see if anonymous ftp is segregated in the network DMZ.	Perform the following to determine if a system is capable of anonymous ftp: # ps –ef |grep ftpd # grep ftp /etc/passwd Ask the SA if the server is on a separate subnet located in a DMZ. If it is not, then this is a finding.	Anonymous FTP is segregated into the network DMZ.			

UNIX-LINUX-156	AC-3, AC-6	Checks to see if the ftp users file is owned by root.	Perform the following on the ftpusers file associated with the applicable operating system: # ls –la <file location> Locations of the ftpusers file: Solaris 5.5.1 – 5.8 /etc/ftpusers Solaris 5.9 –5.10 /etc/ftpd/ftpusers HPUX 10 /etc/ftpusers HPUX 11 /etc/ftpd/ftpusers AIX /etc/ftpusers Linux (wu-ftp) /etc/ftpusers Linux (vsftpd) /etc/vsftpd.ftpusers If the file is not owned by root, then this is a finding.	The ftpusers file is owned by root.			
UNIX-LINUX-157	AC-3, AC-6	The ftpusers file is more permissive than 640.	Perform the following on the ftpusers file associated with the applicable operating system: # ls –la <file location> Locations of the ftpusers file: Solaris 5.5.1 – 5.8 /etc/ftpusers Solaris 5.9 –5.10 /etc/ftpd/ftpusers HPUX 10 /etc/ftpusers HPUX 11 /etc/ftpd/ftpusers AIX /etc/ftpusers Linux (wu-ftp) /etc/ftpusers Linux (vsftpd) /etc/vsftpd.ftpusers If the file is not owned by root, then this is a finding.	The ftpusers file is not more permissive than 640.			
UNIX-LINUX-158	AC-3, AC-6	An ftp users umask is not 077.	To determine the umask of the ftp user, perform the following: # su – ftp # umask If the umask value does not return 077, then this is a finding.	An FTP user’s umask is 077.			

UNIX-LINUX-159	CM-7	Checks to see if File Service Protocol (FSP) is enabled.	To determine if fsp is enabled, perform the following: # grep in.fspd /etc/inetd.conf # netstat –an |grep fspd If an entry for fsp is found, then this is considered a finding.	FSP is disabled.			
UNIX-LINUX-160	AC-3, AC-6	Checks to see if the tftp daemon has the suid or sgid bit set.	Perform : # find / -name “*tftpd” –print to locate the file. Once the file is located, use the command: # ls –la <file location> to check for the suid or sgid bit being set. If either of the bits are set, then this is a finding	The TFTP daemon does not have the suid or sgid bit set.			
UNIX-LINUX-161	AC-3, AC-6	Tftp is not configured to vendor specifications.	Check the /etc/passwd file to determine if TFTP is configured properly: # grep tftp /etc/passwd If a tftp user account does not exist and TFTP is active, then this is a finding. Ensure the user shell is /bin/false or equivalent. If it is not, then this is a finding. Ensure the TFTP user is assigned a home directory. If not, then this is a finding.	TFTP is configured to vendor specifications, including the following: - A TFTP user will be created. - The default shell will be set /bin/false, or equivalent. - A home directory owned by the TFTP user will be created.			

UNIX-LINUX-162	AC-3, AC-6	Tftp is active and it is not documented with the ISSO.	Perform the following to determine if TFTP is active: Solaris, HP-UX, AIX # grep –v “^#” /etc/inetd.conf |grep tftp Solaris 10 # svcs tftp Linux # chkconfig –-list | grep tftp Or # chkconfig tftp If TFTP is found to enabled, ask the SA if it is documented with theI ISSO. This is a finding if it is not documented.	TFTP is disabled OR TFTP is active and justified and documented with the ISSO.			
UNIX-LINUX-163	AC-3, AC-6, AC-17,	Checks to see if a host using Xwindows host writes .Xauthority files or equivalent.	To check for .Xauthority files being utilized, change directory to a user’s home directory and perform: # ls –la .Xauthority If the file does not exist, ask the SA if the user is using Xwindows. If the user is utilizing Xwindows and the .Xauthority file does not exist and host based access control is not being used, then this is a finding.	An X Windows host writes .Xauthority files (or equivalent).			
UNIX-LINUX-164	AC-3, AC-6,	Checks to see if the system is exporting x displays to the world.	Perform the following to determine if access to the X window system is limited to authorized clients: # xhost If the above command returns: “access control disabled, clients can connect from any host”, then this is a finding.	The system is not exporting X displays to the world.			

UNIX-LINUX-165	AC-3, AC-6,	Checks to see if authorized X clients are listed in the X*.hosts file if the .xauthority utility is not used.	Perform the following to determine if the X server is running: # ps –ef |grep X Determine if xauth is being used by: # xauth xauth> list If the above command sequence does not show any host other than the localhost, then xauth is not being used. Search the system for an X*.hosts files, where * is a display number that may be used to limit X window connections. If none are found and user based access control is not being used, then this is a finding.	Authorized X clients are listed in the X*.hosts (or equivalent) file(s) if the .Xauthority utility is not used.			
UNIX-LINUX-166	AC-3, AC-6,	Checks to see if access to the xterminal host is limited to authorized clients.	Perform the following to determine if access to the X window system is limited to authorized clients: # xauth xauth> list Ask the SA if the clients listed are authorized. If they are not, then this is a finding.	Access to the X-terminal host is limited to authorized X clients.			
UNIX-LINUX-167	AC-3,	Checks to see if the xwindows system connections are required If not required, checks to see if they are disabled.	Determine if the X window system is running by: # ps –ef |grep X Ask the SA if the X window system is an operational requirement. If it is not, then this is a finding.	If the Xwindows system connections have been disabled or uninstalled if it is not required for production.			

UNIX-LINUX-168	CM-7	Checks to see if the uucp service is enabled.	Perform the following to determine if uucp is active. Solaris, HP-UX and AIX # grep uucp /etc/inetd.conf Solaris 10 # svcs uucp Linux # chkconfig uucp Or # chkconfig –-list | grep uucp If UUCP is found to be enabled, then this is a finding.	The UUCP service is disabled.			
UNIX-LINUX-169	AC-2, AC-3, IA-2, IA-4,	Checks to see if the snmp community strings have been changed from the default.	Find the snmpd.conf by: # find / -name snmpd.conf –print # more snmpd.conf Search for the community name to check if the password was changed to something other than public, private, snmp-trap or password and which meets the IRS requirements for password construction. The community string will be in plain text.	SNMP community strings have been changed from the default.			
UNIX-LINUX-170	AC-3, AC-6	Checks to see if the Snmpd.conf file is more permissive than 700.	Perform: # find / -name snmpd.conf # ls –lL <snmpd.conf> If the snmpd.conf file is more permissive than 700, then this is a finding.	The snmpd.conf file is not more permissive than 700.			

UNIX-LINUX-171	AC-3, AC-6	Checks to see if the mib files are more permissive than 640.	Perform the following to find all the Management Information Base (MIB) files on the system: # find / -name *.mib –print # ls –lL <mib file> Any file returned with permissions greater than 640 is a finding.	The MIB files are not more permissive than 640.			
UNIX-LINUX-172	AC-3, AC-6	Checks to see if the snmpd.conf file is not owned by root and group owned by sys or the application.	Perform: # find / -name snmpd.conf # ls –lL <snmpd.conf> # find / -name *.mib If the snmpd.conf file is not owned by root and group owned by sys or the application, then this is a finding.	The snmpd.conf and .mib files are owned by root and group owned by sys or the application.			
UNIX-LINUX-173	CM-7	Checks to see if Snmp does runs on dedicated hardware.	To check if SNMP is used, execute the following command: # netstat -a | grep LISTEN | grep snmp. # netstat –a | grep LISTEN | egrep “161|162” If there is any output, then ask the SA if this is an snmp server. If it is an snmp server, then ask what other applications run on it. If there is anything other than network management software and DBMS software that is used only for the storage and inquiry of snmp data, this is a finding.	SNMP runs on dedicated hardware.			
UNIX-LINUX-174	SC-2	Checks to see if the information system separates user functionality (including user interface services) from information system management functionality.	Interview the SA or ISSO and ask if the information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.	The information system separates user functionality (including user interface services) from information system management functionality.			
UNIX-LINUX-175	AC-3, AC-5, AC-6	Checks to see if the /etc/syslog.conf is owned by root or is more permissive than 640.	Check /etc/syslog.conf ownership and permissions: # ls –lL /etc/syslog.conf If /etc/syslog.conf is not owned by root or is more permissive than 640, then this is a finding.	The /etc/syslog.conf file is owned by root or is not more permissive than 640.			

UNIX-LINUX-176	AC-3, AC-6,	The /etc/syslog.conf group owner is root, bin, or sys.	Check /etc/syslog.conf group ownership: # ls –lL /etc/syslog.conf If /etc/syslog.conf is not group owned by root, sys, or bin, then this is a finding.	The /etc/syslog.conf file is group owned by root, sys, or bin.			
UNIX-LINUX-177	AC-4,	A system using a remote loghost is not documented with the ISSO.	Perform the following to determine if the system is using a remote loghost: # grep loghost /etc/hosts If the loghost entry is a remote machine, then ask the SA if the remote machine is documented as a loghost with the ISSO. If it is not documented then this is a finding.	A system is using a remote loghost and is documented with the ISSO.			
UNIX-LINUX-178	AC-4, IA-7	Checks to see if SSH, or a similar utility is running and SSHv1 compatibility is used.	Locate the sshd_config file: # find / -name sshd_config # more <sshd_config file location> Examine the file. If the variables 'Protocol 2,1' or, 'Protocol 1' are defined on a line without a leading comment, this is a finding. If the SSH server is F-Secure, the variable name for SSH 1 compatibility is 'Ssh1Compatibility', not 'protocol'. If the variable 'Ssh1Compatiblity' is set to 'yes', then this is a finding.	SSH is not using v1 compatibility, only v2 connections are accepted.			
UNIX-LINUX-179	AC-4, AC-5,	Checks to see if the system is a router, if it is not a router, the default gateway must be set.	Perform the following to determine if a default route is defined: # netstat –r |grep default If a default route is not defined, then this is a finding.	The system is not a router and has a default gateway defined.			
UNIX-LINUX-180	AC-4, AC-5,	Checks to see if routing is implemented on dedicated hardware. If not it should be and documented with the ISSO.	Perform the following to determine if the systems is used for routing: # netstat –a | grep –i listen | grep route Ask the SA if the system is used for any other services such as web servers, file servers, DNS servers, or applications servers. If it is used for another service, then this is a finding.	Routing is implemented on dedicated hardware. If not, it is documented with the ISSO.			

UNIX-LINUX-181	AC-3, AC-6	Checks to see if the export configuration file is owned by root.	− Solaris # ls –lL /etc/dfs/dfstab − HP-UX # ls –lL /etc/exports − AIX # ls –lL /etc/exports − Linux # ls –lL /etc/exports If the export configuration file is not owned by root, then this is a finding.	The export configuration file is owned by root.			
UNIX-LINUX-182	AC-3, AC-6	Checks to see if the export configuration file is more permissive than 644.	− Solaris # ls –lL /etc/dfs/dfstab − HP-UX # ls –lL /etc/exports − AIX # ls –lL /etc/exports − Linux # ls –lL /etc/exports If the export configuration file is more permissive than 644, then this is a finding.	The export configuration file has permissions less than or equal to 644.			
UNIX-LINUX-183	AC-3, AC-6,	Checks to see if NFS files systems exported as writeable have been justified and documented by the ISSO.	Perform the following to determine if NFS File Systems are writeable: # exportfs –v |grep rw If any entries are returned, ask the SA if the file systems have been approved and documented with the ISSO for export as writable.	NFS file systems exported as writeable have been justified and documented by the ISSO.			

UNIX-LINUX-184	AC-3, AC-6	Checks to see if NFS exported system files and directories are owned by root.	Perform the following to check for NFS exported files systems: # exportfs –v This will display all of the exported file systems. For each file system displayed perform and check the ownership: # ls –lL <filesystem> If the files and directories are not owned by root, then this is a finding.	NFS exported system files and system directories are owned by root.			
UNIX-LINUX-185	AC-3, IA-2, IA-4	Checks to see if the NFS server is configured to deny client access request that do not include a user id.	Perform the following to determine if the 'anon' option is set correctly for exported file systems: # exportfs –v |grep anon Each of the exported file systems should include an entry to check for the 'anon= 'option being set to –1 or an equivalent (60001, 65534, or 65535). Linux systems use the 'anonuid' option instead of 'anon'. Note: If the anon flag is found to have a UID of 0, this finding is elevated to a Severity Code I.	The NFS server is configured to deny client access requests that do not include a userid.			
UNIX-LINUX-186	AC-6, AC-17, AC-3, AC-17,	Checks to see if the NFS server is configured to restrict file system access to local hosts.	Perform the following to check for access permissions: # exportfs –v If the exported filesystems do not contain the 'rw' or 'ro' options, then this is a finding.	The NFS server is configured to restrict filesystem access to local hosts.			

UNIX-LINUX-187	AC-3, IA-2, IA-4	Checks to see if the SA ensures that the sec option is not set to none and the default authentication is not set to none.	This check only applies to Solaris. Perform the following on NFS servers: # grep “^default” /etc/nfssec.conf Check to ensure the second column does not equal ‘0’. This would indicate the default is set to none. Perform the following to check currently exported file systems: # more /etc/exports Or # more /etc/dfs/dfstab If the option ‘sec=none’ is set on any of the exported file systems, then this is a finding.	The sec option is not set to none (or equivalent); additionally the default authentication is not set to none.			
UNIX-LINUX-188	AC-3.	Checks to see if the root access option for nfs has been authorized and documented with the ISSO.	Perform the following to determine if the NFS server is exporting with the root access option: # exportfs –v | grep “root=” If the option is found on an exported file system, ask the SA if the access is justified and documented with the ISSO. If it is not, then this is a finding.	The root access option for NFS has been justified and documented with the ISSO.			
UNIX-LINUX-189	AC-3, AC-6	Checks to see if the nosuid and nosgid options are enabled on an nfs client.	Perform the following to determine if nfs clients are mounting file systems with the nosuid and nosgid options: # mount –v | grep " type nfs " | grep "nosuid" # mount –v | grep " type nfs " | grep "nosgid" If the mounted file systems do not have the above two options, then this is a finding and it must be justified and documented with the ISSO.	The nosuid and nosgid options are enabled on a NFS Client.			
UNIX-LINUX-190	CM-7	Checks to see if a public instant messaging client is installed.	If an IM client is installed, ask the SA if it configured to communicate only with IRS IM servers. If it has access to servers on the internet, then this is a finding. EXAMPLES - GAIM, PIDGIN, KOPETE (or others) #rpm -qa |grep -i gaim #rpm -qa |grep -I pidgin or find / -name gaim find / -name pidgin find / -name kopete	A public instant messaging client is not installed.			

UNIX-LINUX-191	CM-7	A peer-to-peer file sharing application is installed and not authorized and documented with the DAA.	Ask the SA if any peer-to-peer file-sharing applications are installed. Some examples of these applications include: - Napster - Kazaa - ARES - Limewire - IRC Chat Relay - BitTorrent If any of these applications are installed without an Acceptance of Risk Letter from the DAA, then this is a finding.	A peer-to-peer file-sharing application is installed and is authorized and documented with the DAA.			
UNIX-LINUX-192	CM-7	Checks to see if Samba is running and is not being used.	Perform the following to determine if the Samba server is running: # ps –ef |grep smbd If a process is returned as running, ask the SA if the Samba server is operationally required. If it is not, then this is a finding.	Samba is not running or is running and is operationally required.			
UNIX-LINUX-193	AC-4,	Checks to see if the Samba web administration tool is used with SSH port forwarding.	SWAT must be utilized with ssh to ensure a secure connection between the client and the server. The ssh daemon on the server must be configured to allow port forwarding. If SWAT is being utilized to administer Samba on the server, perform the following: # grep AllowTcpForwarding /etc/ssh/sshd_config If the line is commented out or set to 'no' and SWAT is in use, then this is a finding.	The Samba Web Administration tool is used with SSH port forwarding.			
UNIX-LINUX-194	AC-3, AC-6	Checks to see if the /etc/smb.conf file is owned by root.	Check /etc/samba/smb.conf ownership: # ls –lL /etc/samba/smb.conf If /etc/samba/smb.conf is not owned by root, then this is a finding.	The smb.conf file is owned by root.			

UNIX-LINUX-195	AC-3,	Checks to see if the /etc/smb.conf file is group owned by root.	Check /etc/samba/smb.conf permissions: # ls –lL /etc/samba/smb.conf If /etc/samba/smb.conf is not group owned by root, then this is a finding.	The smb.conf file is group owned by root.			
UNIX-LINUX-196	AC-3, AC-6	Checks to see if the /etc/smb.conf is more permissive than 644.	Check /etc/samba/smb.conf permissions: # ls –lL /etc/samba/smb.conf If /etc/samba/smb.conf is more permissive than 644, then this is a finding.	The smb.conf file is equal to or less permissive than 644.			
UNIX-LINUX-197	AC-3, AC-6	Checks to see if the smb password file is owned by root.	Check /etc/samba/smbpasswd ownership: # ls –lL /etc/samba/smbpasswd If /etc/samba/smbpasswd is not owned by root, then this is a finding.	The smbpasswd file is owned by root.			
UNIX-LINUX-198	AC-3, AC-6	Checks to see if the /etc/smbpasswd file is group owned by root.	Check /etc/samba/smbpasswd ownership: # ls –lL /etc/samba/smbpasswd If /etc/samba/smbpasswd is not group owned by root, then this is a finding.	The smbpasswd file is group owned by root.			
UNIX-LINUX-199	AC-3, AC-6	Checks to see if the /etc/smbpasswd file is more permissive than 600.	Check /etc/samba/smbpasswd permissions: # ls –lL /etc/samba/smbpasswd If /etc/samba/smbpasswd is more permissive than 600, then this is a finding.	The smbpasswd file is equal to or less permissive than 600.			
UNIX-LINUX-200	CM-7	Checks to see if the server is a internet network news server; if so, it checks to see if it has been authorized and documented by the ISSO.	Perform: # ps –e | egrep “innd|nntpd” If an Internet Network News server is running and not justified and documented by the ISSO, then this is a finding.	Any servers running the Internet Network News server are justified and documented by the ISSO.			

UNIX-LINUX-201	AC-3, AC-6	Checks to see if the /etc/news/hosts.nntp file is more permissive than 600.	Check /etc/news/hosts.nntp permissions: # ls –lL /etc/news/hosts.nntp If /etc/news/hosts.nntp is more permissive than 600, then this is a finding.	The /etc/news/hosts.nntp file is less permissive than 600.			
UNIX-LINUX-202	AC-3, AC-6	Checks to see if the /etc/news/nntp.nolimit file is more permissive than 600.	Check /etc/news/hosts.nntp.nolimit permissions: # ls –lL /etc/news/hosts.nntp.nolimit If /etc/news/hosts.nntp.nolimit is more permissive than 600, then this is a finding.	The /etc/news/hosts.nntp.nolimit file has permissions that are less than or equal to 600.			
UNIX-LINUX-203	AC-3, AC-6	Checks to see if the /etc/news/nnrp.access file is more permissive than 600.	Check /etc/news/nnrp.access permissions: # ls –lL /etc/news/nnrp.access If /etc/news/nnrp.access is more permissive than 600, then this is a finding.	The /etc/news/nnrp.access file has permissions that are less than or equal to 600..			
UNIX-LINUX-204	AC-3, AC-6	Checks to see if the /etc/news/passwd/nntp file is more permissive than 600.	Check /etc/news/passwd.nntp permissions: # ls –lL /etc/news/passwd.nntp If /etc/news/passwd.nntp is more permissive than 600, then this is a finding.	The /etc/news/passwd.nntp file has permissions that are less than or equal to 600..			
UNIX-LINUX-205	AC-3, AC-6	Checks to see if the files in /etc/news are owned by root or news.	Check /etc/news files ownership: # ls –al /etc/news If /etc/news files are not owned by root or news, then this is a finding.	The files contained in the /etc/news directory are owned by root or news.			
UNIX-LINUX-206	AC-3, AC-6	Checks to see if the /etc/news files group owner is root or news.	Check /etc/news files group ownership: # ls –al /etc/news If /etc/news files are not group owned by root or news, then this is a finding.	The files contained in the /etc/news directory are group owned by root or news.			

UNIX-LINUX-207	CM-7	Checks to see if NIS is implemented under udp.	# rpcinfo -p | grep yp | grep udp If NIS/NIS+ is implemented under UDP, then this is a finding.	NIS/NIS+ is not implemented under UDP.			
UNIX-LINUX-208	CM-7	Checks to see if the NIS protocol is in use and is justified and documented with the ISSO.	Peform the following to determine if NIS is active one the system: # ps –ef |grep ypbind If NIS is found active on the system, ask the SA if it's use is documented with the ISSO. If NIS use is not documented, this is a finding.	The NIS protocol is in use and justified and documented with the ISSO.			
UNIX-LINUX-209	SI-3	Checks to see if a system vulnerability tool is being run on the system weekly, or at an interval that is compliant with IRS security policy.	Perform the following to check for a security tool executing monthly: # crontab –l Check for the existance of a vulnerability assessment tool being scheduled and run monthly. If no entries exist in the crontab, ask the SA if a vulnerability tool is run monthly. In addition, if the tool is run monthly, ask to see any reports that may have been generated from the tool. If a tool is not run monthly, then this a finding.	A system vulnerability assessment tool is being run on the system weekly, or at an interval that is compliant with IRS security policy.			
UNIX-LINUX-210	AC-13, AU-5, AU-6, AU-7	Checks to see if the system vulnerability assessment tool and file system integrity baseline tool notify the SA of a security breach.	Perform: find / -name (program name) –print to check for the existance of security tools on the system. Ask the SA if the program is configured to notify the ISSO and SA if a breach is detected. This check must be justified and documented with the ISSO. Tripwire is a common system integrity checker.	The system vulnerability assessment tool and file system integrity baseline tool notifies the SA and the ISSO of a security breach or a suspected security breach.			

UNIX-LINUX-211	AC-2, AC-3,AC-6, AC-17, IA-3	Checks to see if an access control program is being used.	To determine if tcp wrappers is installed perform the following: Solaris, HP-UX , and AIX # grep tcpd /etc/inetd.conf Solaris 10 # svcprop –p defaults inetd | grep tcp_wrappers This should return a line with the following: defaults/tcp_wrappers boolean true If the above line contains the word false, then this is a finding on Solaris 10. Solaris 8 or 9 # grep –i enable_tcpwrappers /etc/default/inetd If the value returned is not set to yes and /etc/inetd.conf does not contain tcpd, then this is a finding. Linux # rpm –qa |grep tcpd or Check the services in the /etc/xinetd.d directory that are not disabled for an entry containing noaccess or only_from. Ensure an entry returns specifically for tcpd, not tcpdump.	An access control program is being used.			

UNIX-LINUX-212	SC-5	The information system protects against or limits the effects of the following types of denial of service attacks	Perform the following to ensure the network security settings are enabled for each operating system. The command is listed with the expected response next to it in parenthesis. Solaris # ndd /dev/ip ip_forward_src_routed (0) # ndd /dev/tcp tcp_rev_src_routes (0) # ndd /dev/tcp tcp_conn_req_max_q0 (2048 or greater) # ndd /dev/tcp tcp_conn_req_max_q (1024) # ndd /dev/ip ip_respond_to_timestamp (0) # ndd /dev/ip ip_respond_to_echo_broadcast (0) # ndd /dev/ip ip_respond_to_timestamp_broadcast (0) HP-UX # ndd /dev/ip ip_forward_src_routed (0) # ndd /dev/ip ip_respond_to_timestamp (0) # ndd /dev/ip ip_respond_to_echo_broadcast (0) # ndd /dev/ip ip_respond_to_timestamp_broadcast (0) AIX # /usr/sbin/no –o ipsrcroutesend (0) # /usr/sbin/no –o directed_broadcast (0) # /usr/sbin/no –o bcastping (0) # /usr/sbin/no –o ipsrcrouteforward (0) Linux # sysctl –a | grep net.ipv4.ip_forward (0) # sysctl –a | grep net.ipv4.tcp_max_syn_backlog (1280) # sysctl –a | grep net.ipv4.conf.all.accept_source_route (0) # sysctl –a | grep net.ipv4.icmp_echo_ignore_broadcasts (1) If any of the above settings are not applied, then this is a finding.	UNIX host is configured to be resiliant against denial of service attacks.			
UNIX-LINUX-213	SC-8	Checks to see if the organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.	Interview the SA or ISSO and determine if a file integrity utility such as md5 or Sha is used to verify the check sums of files before and after transit.	The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.			

UNIX-LINUX-214	SC-9, SC-23	Checks to see if the organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures	Interview the SA or ISSO to determine if all connections to the server are via *HTTPS using SSL3.1 or TLS *SSH or SCP v2 only *Other communications methods using tunneling via OpenSSL or equivalent FIPS encryption.	The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures			
UNIX-LINUX-215	SC-13	Checks to see that when information requires cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.	Interview the SA or ISSO to determine if FIPS 140-2 encryption is used on items requiring the use of cryptography for protection.	For information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with FIPS-140-2, applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.			
UNIX-LINUX-216	AC-2, AC-3, AC-13, AU-6	Checks to see if the access control program logs each system access attempt.	Normally tcpd logs to the mail or daemon facility in /etc/syslog.conf. Perform the following to determine if syslog is configured to log events by tcpd. # more /etc/syslog.conf Look for entries similar to the following: mail.debug /var/adm/maillog mail.none /var/adm/maillog mail.* /var/log/mail or maillog auth.info /var/log/messages daemon.* /var/log/messages authpriv /var/log/secure The above entries would indicate mail alerts are being logged. If no entries for mail exist, then tcpd is not logging and this is a finding.	The access control program logs each system access attempt.			

UNIX-LINUX-217	AC-2, AC-3, AC-6, AC-17, IA-3	Checks to see if the access control program is configured to grant and deny system access to specific hosts.	Check for the existence of /etc/hosts.allow and /etc/hosts.deny: # ls –la /etc/hosts.allow # ls –la /etc/hosts.deny # grep “ALL: ALL” /etc/hosts.deny If the ‘ALL: ALL’ is in the /etc/hosts.deny file, then any tcp service from a host or network not listed in the /etc/hosts.allow file will not be allowed access. If the entry is not in /etc/hosts.deny or if either of the two files do not exist, then this is a finding.	The access control program is configured to grant and deny system access to specific hosts.			
UNIX-LINUX-218	SI-3	Checks to see if an IRS approved virus scan program is used or configured correctly.	Check for the existance of an antivirus program running on the UNIX host. Popular anti-virus programs such as Mcafee's command line scanner or ClamAV should be used on UNIX servers that run file sharing services for Windows such as Samba, NFS (services for UNIX), FTP, or servers that that transmit files to Windows hosts such as SMTP/IMAP-POP servers or any other service that allows for files to be shared/stored for and by Windows users. Check if AV sevices are scheduled to run: For ClamAV #ps -ef |grep clamd #find / -name freshclam.conf and check for update intervals. For Mcafee command line scanner Solaris # grep uvscan /var/spool/cron/crontabs/* HP-UX # grep uvscan /var/spool/cron/crontabs/* AIX # grep uvscan /var/spool/cron/crontabs/* Linux # grep uvscan /var/spool/cron/* # grep uvscan /etc/cron.d/* # grep uvscan /etc/cron.daily/* # grep uvscan /etc/cron.hourly/* # grep uvscan /etc/cron.monthly/* # grep uvscan /etc/cron.weekly/* Perform the following to ensure the virus definition signature files are not older than 14 days. # ls –la clean.dat names.dat scan.dat If a virus scanner is not being run weekly or the virus definitions are older than 14 days, then this is a finding.	An IRS approved virus scan program is used and configured correctly.			
SOLARIS SPECIFIC CHECKS BELOW							

SOLAIRS-SPECIFIC-1	AC-2, AC-3,	Checks to see if the audit_user file has a different auditing level for specific users.	Perform: # more /etc/security/audit_user If /etc/security/audit_user has entries other than root, ensure the users defined are audited with the same flags as all users as defined in /etc/security/audit_control file.	The audit_user file has the same auditing level for all users.			
SOLAIRS-SPECIFIC-2	AC-3, AC-6,AU-9	Checks to see if the audit_user is owned by root.	Check /etc/security/audit_user ownership: # ls –lL /etc/security/audit_user If /etc/security/audit_user is not owned by root, then this is a finding.	The audit_user file is owned by root.			
SOLAIRS-SPECIFIC-3	AC-3, AC-6,AU-9	Checks to see if the audit_user file is group owned by root, sys, or bin.	Check /etc/security/audit_user group ownership: # ls –lL /etc/security/audit_user If /etc/security/audit_user is not group owned by root, sys, or bin, then this is a finding.	The audit_user file is group owned by root, sys, or bin.			
SOLAIRS-SPECIFIC-4	AC-3, AC-6,AU-9	Checks to see if the audit _user file is more permissive than 640.	Check /etc/security/audit_user permissions: # ls –lL /etc/security/audit_user If /etc/security/audit_user is more permissive than 640, then this is a finding.	The audit_user file has permissions of less or equal to 640.			
SOLAIRS-SPECIFIC-5	AC-3,	Checks to see if the ASET master files are located in the /usr/aset/masters directory.	Verify that ASET is being used by: # crontab –l |grep aset If there is an output, then check to make sure that the files in question are in the /usr/aset/masters directory by performing: # ls –l /usr/aset/masters The following files should be in the listing: tune.high, tune.low, tune.med, and uid_aliases. If the all of the files are not in the directory listing, then this is a finding.	Aset master files are located in the /usr/aset/masters directory.			

SOLAIRS-SPECIFIC-6	AC-3,	Checks to see if the /usr/aset/masters/uid_aliases is empty.	# more /usr/aset/masters/uid_aliases If fhe /usr/aset/masters/uid_aliases file is not empty or all contents are not commented out, then this is a finding.	The /usr/aset/masters/uid_aliases file is empty.			
SOLAIRS-SPECIFIC-7	AC-3,	Checks to see if ASET is used on a firewall system and the firewall parameters are in /usr/aset/asetenu.	Peform the following to determine if ASET is being used: # crontab –l |grep aset An a returned entry would indicate ASET is being utilized. Determine if ASET is configured to check firewall settings by: # grep TASKS /usr/aset/asetenv | grep firewall If an entry is not returned, then this is a finding.	ASET is not used on any firewall system and the firewall parameters are in /usr/aset/asetenv.			
SOLAIRS-SPECIFIC-8	AC-3,	Checks to see if the ASET environment variables in the asetenv file are correct.	Determine is ASET is being used by: # crontab –l | grep aset Check the configuration of ASET by: # more /usr/aset/asetenv If there are any changes below the following two lines that are not comments, this is a finding: # Don't change from here on down ... # # there shouldn't be any reason to. # In addition, if any of the following lines do not match, this is a finding. TASKS="firewall env sysconf usrgrp tune cklist eeprom" CKLISTPATH_LOW=${ASETDIR}/tasks:${ASETDIR} \ /util:${ASETDIR}/masters:/etc CKLISTPATH_MED=${CKLISTPATH_LOW}:/usr/bin:/usr/ucb CKLISTPATH_HIGH=${CKLISTPATH_MED}:/usr/lib:/sbin: \ /usr/sbin:/usr/ucblib YPCHECK=false PERIODIC_SCHEDULE="0 0 * * *" UID_ALIASES=${ASETDIR}/masters/uid_aliases	ASET environment variables in the asetenv file are correct.			

SOLAIRS-SPECIFIC-9	AC-3,	Checks to see if NIS+ is configured on the solaris system and ypcheck is set to true.	Perform the following to determine if ASET is configured to check NIS+: # grep YPCHECK /usr/aset/asetenv If NIS+ is running and the YPCHECK variable is set to false, then this is a finding.	NIS+ is not configured on the Solaris system and YPCHECK is set to true.			
SOLAIRS-SPECIFIC-10	AC-2, AC-3,	Checks to see if the /usr/aset/userlist file contains a list of all system users.	Perform the following to determine if ASET is scheduled to run: # crontab –l | grep aset The default user list is /usr/aset/userlist. If the –u option is specified in the crontab entry, then the userlist file is the argument supplied to the –u option. Perform: # more /usr/aset/userlist If the file does not exist or if the file does not contain a list of the system usernames, then this is a finding.	The /usr/aset/userlist file contains a list of all system users.			
SOLAIRS-SPECIFIC-11	AC-3, AC-5, AC-6	Checks to see if the /usr/aset/userlist file is owned by root.	# ls –lL /usr/aset/userlist If /usr/asset/userlist is not owned by root, then this is a finding.	The /usr/aset/userlist file is owned by root.			
SOLAIRS-SPECIFIC-12	AC-2, AC-3, AC-5, AC-6	Checks to see if the /user/aset/userlist file is more permissive than 600.	# ls –lL /usr/aset/userlist If /usr/aset/userlist is more permissive than 600, then this is a finding.	The /usr/aset/userlist file has permission of less than or equal to 600.			

SOLAIRS-SPECIFIC-13	SA-10,	Checks for a version of the Sun Answerbook2 that was found vulnerable to the dwhttpd format string vulnerability.	Applicable to Solaris 2.5.1 through Solaris 5.8. # find / -name dhttpwd If the Answerbook binary is found, check for the following patches: Solaris 5.5.1 110532-01 Solaris 5.5.1_x86 110538-01 Solaris 5.6 110532-01 Solaris 5.6_x86 110538-01 Solaris 5.7 110532-01 Solaris 5.7_x86 110538-01 Solaris 5.8 110532-01 Solaris 5.8_x86 110538-01 - Apply the applicable patch or remove the binary/application to remediate this finding. - Or, the vulnerable binary may be renamed and the permissions modified to 000 to downgrade the finding, to LOW	Sun AnswerBook2 has no vulnerabilities to the dwhttpd format string.			
SOLAIRS-SPECIFIC-14	AU-2	Checks to see if the NFS server does have logging implemented.	To enable NFS server logging the 'log' option must be applied to all exported files systems in the /etc/dfs/dfstab. Perform the following to verify NFS is enabled: # share The preceding command will display all exported filesystems. Each line should contain a 'log' entry to indicate logging is enabled. If the 'log' entry is not present then this is a finding. If the share command does not return anything, then this is not an NFS server and this is considered Not Applicable.	All NFS servers have logging implemented.			
HP-UX SPECIFIC CHECKS BELOW							
HP-UX SPECIFIC-1	AC-3, AC-13, AU-3, AU-6, AU-8	Checks to see if the HPUX audomon_args flag is set to IRS or other more secure settings.	Determine if the following flags are set for auditing: # tail /etc/rc.config.d/auditing The AUDOMON_ARGS flag should be the last line in the file. Look at the arguments and compare them to -p 20, -t 1, -w 90. If any of these differ, this a finding.	HP-UX AUDOMON_ARGS flag is set to IRS or other best practice documents. More secure settings should be similar to: -p 20, -t 1, -w 90.			

HP-UX SPECIFIC-3	AC-3, AC-6	Checks to see if the /etc/securetty is owned by root.	# ls –lL /etc/securetty If /etc/securetty is not owned root, then this is a finding.	The /etc/securetty file is owned by root.			
HP-UX SPECIFIC-4	AC-3, AC-6	Checks to see if the /etc/securetty file is group owned by root, sys, or bin.	# ls –lL /etc/securetty If /etc/securetty is not grup owned by root, sys, or bin, then this is a finding.	The /etc/securetty file is group owned by root, sys, or bin.			
HP-UX SPECIFIC-5	AC-3, AC-6	Checks to see if the /etc/securetty is more permissive than 640.	# ls –lL /etc/securetty If /etc/securetty is more permissive than 640, then this is a finding.	The /etc/securetty file has permissions of less than or equal to 640.			
AIX-SPECIFIC-CHECKS							
AIX-SPECIFIC-1	CM-7	Checks to see if the securetcpip command has been used.	The securetcpip command is in /etc. If it is not there, this is a finding. Perform: # more /etc/security/config If the stanza: tcpip: netrc = ftp, rexec is not there, then this is a finding. The stanza indicates the securetcpip command, which disables all the unsafe tcpip commands, (e.g., rsh, rlogin, tftp)has been executed.	The securetcpip command has been used.			
LINUX-SPECIFIC-CHECKS							
LINUX-SPECIFIC-1	AC-3,	Checks to see if the CMOS is configured to disable the capability to boot from removable media.	If the CMOS is not configured to disable the capability to boot from removable media (e.g., diskette), then this is a finding.	The CMOS is configured to disable the capability to boot from removable media (e.g., diskette).			
LINUX-SPECIFIC-2	AC-3,	Checks to see if the password configuration table has the supervisor passwd set to off or the user passwd set to on.	On x86 systems enter the system BIOS and confirm that a supervisor password is enabled. Some systems will have only one password setting, while others may have both user and supervisor settings. On those with two settings, ensure the supervisor password is enabled and set. If the system cannot be rebooted to confirm the settings, ask the system administrator if a BIOS password is enabled. If it is not, then this is a finding.	The Password Configuration Table has the Supervisor Password set to ON or the User Password set to OFF.			

LINUX-SPECIFIC-3	AC-6, AC-3	Checks to see if the grub.conf file is more permissive the 600.	Check /etc/grub.conf permissions: # ls –lL /etc/grub.conf If /etc/grub.conf is more permissive than 600, then this is a finding	The grub.conf is less permissive than 600.			
LINUX-SPECIFIC-4	AC-6, AC-3	Checks to see if the /etc/lilo.conf is more permissive than 600.	Check /etc/lilo.conf permissions: # ls –lL /etc/lilo.conf If /etc/lilo.conf is more permissive than 600, then this is a finding.	The /etc/lilo.conf file is less permissive than 600.			
LINUX-SPECIFIC-5	CM-7	Checks to see if Kickstart or Autoyast are used outside an isolated development lan.	On SuSE systems tftp must be running for AutoYaST to work properly. Check for tftp by: # chkconfig –-list tftp If tftp is found, as the SA if the server is configured for AutoYaST. Redhat systems utilize nfs and bootp to assist Kickstart. Perform: # more /etc/exports # more /etc/bootptab and ask the SA if any of the exported file systems contain Kickstart images to be installed on a client.	Kickstart or AutoYaST are not used outside an isolated development LAN.			
LINUX-SPECIFIC-6		Checks to see if the linux system is capable of booting multiple operating systems and is not documented with the ISSO.	Review the applicable boot loader configuration file to ensure it is capable of booting only one operating system. For the grub boot loader, /etc/grub.conf should be reviewed. For the lilo boot loader, /etc/lilo.conf should be reviewed. Locations for these file may differ on older versions of linux.	A Linux system capable of booting multiple operating systems is justified and documented with the ISSO.			
LINUX-SPECIFIC-7	CM-7	Checks to see if the rpc.ugidd daemon is enabled.	To check for the rpc.ugidd daemon perform: # chkconfig –list rpc.ugidd Or # ps –ef | grep –i ugidd If the daemon is running or installed this is a finding.	The rpc.ugidd daemon is not enabled.			

LINUX-SPECIFIC-8	AC-2, AC-3, AC-6	Checks to see if special privileged accounts such as shutdown and halt have been deleted.	Perform the following to check for unnecessary privileged accounts: # more /etc/passwd Some examples of unnecessary privileged accounts include halt, shutdown, reboot and who.	Special privilege accounts, such as shutdown and halt, have been deleted.			
LINUX-SPECIFIC-9	AC-2, AC-3	Unnecessary accounts and associated software have not been deleted.	Perform the following to check for unnecessary user accounts: # more /etc/passwd Some examples of unnecessary accounts includes games, news, gopher, ftp.	Unnecessary accounts (e.g., games, news) and associated software have been deleted.			
LINUX-SPECIFIC-10	AC-17	Checks to see if the X server has the correct options enabled.	X servers get started several ways, such as xdm, gdm or xinit. Perform: # ps –ef |grep X Output for example: /usr/X11R6/bin/X –nolisten –ctp –br vt7 –auth /var/lib/xdm/authdir/authfiles/A:0 Check the Xservers file to ensure the following options are enabled: -audit, -auth. Xserver files can found in: /etc/X11/xdm/Xservers /etc/opt/kde3/share/config/kdm/Xservers /etc/X11/gdm/Xservers	The X server has the correct options enabled.			

LINUX-SPECIFIC-11	AC-17	Checks to see if the Xserver has one of the following options enabled: -ac, -core, -nolock.	X servers get started several ways, such as xdm, gdm or xinit. Perform: # ps –ef |grep X Output for example: /usr/X11R6/bin/X –nolisten –ctp –br vt7 –auth /var/lib/xdm/authdir/authfiles/A:0 The above example show xdm is controlling the Xserver. Check the Xservers file to ensure the following options are not enabled: -ac, -core, and -nolock . Xserver files can found in: /etc/X11/xdm/Xservers /etc/opt/kde3/share/config/kdm/Xservers /etc/X11/gdm/Xservers	The X server has none of the following options enabled: -ac, -core (except for debugging purposes), or -nolock.			
LINUX-SPECIFIC-12	AC-3, AC-6	Checks the /etc/login.access or /etc/security/access.conf is owned by root.	Check file applicable to the system, login.access or access.conf. Check /etc/login.access ownership: # ls –lL /etc/login.access Check /etc/security/access.conf ownership: # ls –lL /etc/security/access.conf If /etc/login.access or /etc/security/access.conf is not owned by root, then this is a finding.	The /etc/login.access or /etc/security/access.conf file is owned by root.			

LINUX-SPECIFIC-13	AC-3, AC-6	Checks to see if the /etc/login.access or /etc/security/access.conf is group owned by root.	Check file applicable to the system, login.access or access.conf. . Check /etc/login.access ownership: # ls –lL /etc/login.access Check /etc/login.access ownership: # ls –lL /etc/security/access.conf If /etc/login.access or /etc/security/access.conf is not group owned by root, then this is a finding.	The /etc/login.access or /etc/security/access.conf file is group owned by root.			
LINUX-SPECIFIC-14	AC-3, AC-6, AC-3,	Checks to see if the /etc/login.access or /etc/security/access.conf file is more permissive than 640.	Check file applicable to your system, login.access or access.conf. . Check /etc/login.access ownership: # ls –lL /etc/login.access Check /etc/login.access ownership: # ls –lL /etc/security/access.conf If /etc/login.access or /etc/security/access.conf is more permissive than 640, then this is a finding.	The /etc/login.access or /etc/security/access.conf file has permissions less than or equal to 640.			
LINUX-SPECIFIC-15	AC-3, AC-6	Checks to see if the /etc/sysctl.conf file is not owned by root.	Check /etc/sysctl.conf ownership: # ls –lL /etc/sysctl.conf or # ls –lL /etc/sysconfig/sysctl If /etc/sysctl.conf is not owned by root, then this is a finding.	The /etc/sysctl.conf file is owned by root.			
LINUX-SPECIFIC-16	AC-3, AC-6	Checks to see if the /etc/sysctl.conf is group owned by root.	Check /etc/sysctl.conf group ownership: # ls –lL /etc/sysctl.conf If /etc/sysctl.conf is not group owned by root, then this is a finding.	The /etc/sysctl.conf file is group owned by root.			

LINUX-SPECIFIC-17	AC-3, AC-6	Checks to see if the /etc/sysctl.conf is more permissive than 600.	Check /etc/sysctl.conf permissions: # ls –lL /etc/sysctl.conf If /etc/sysctl.conf is more permissive than 600, then this is a finding.	The /etc/sysctl.conf file has permissions less than or equal to 600.			
LINUX-SPECIFIC-18	CM-7	Checks to see if the nfs insecure option is set.	Determine if an NFS server is running on the system by: # ps –ef |grep nfsd If an NFS server is running, confirm that it is not configured with the insecure option by: # exportfs –v The example below would be a finding: /misc/export speedy.redhat.com(rw,insecure)	The insecure option is not set.			
LINUX-SPECIFIC-19	CM-7	Checks to see if the insecure_locks option is set.	Determine if an NFS server is running on the system by: # ps –ef |grep nfsd If an NFS server is running, confirm that it is not configured with the insecure_locks option by: # exportfs –v The example below would be a finding: /misc/export speedy.redhat.com(rw,insecure_locks)	The insecure_locks option is not set.			
LINUX-SPECIFIC-20	AC-3	Checks to see if the Linux X86 CTRL-ALT-DEL key sequence has been disabled.	Verify that Linux systems have disabled the <CTRL><ALT><DELETE> key sequence by performing: # grep ctrlaltdel /etc/inittab If the line returned is not commented out then this is a finding.	The Ctrl-Alt-Delete sequence is disabled and the system is located in a controlled access area accessible only by SAs.			
LINUX-SPECIFIC-21	AC-3, AC-5, AC-6	Checks to see if the /etc/securetty file is group owned by root, sys, or bin.	eck /etc/securetty group ownership: # ls –lL /etc/securetty If /etc/securetty is not group owned by root, sys, or bin, then this is a finding.	The /etc/securetty file is group owned by root, sys, or bin.			

LINUX-SPECIFIC-22	AC-3, AC-6	Checks to see if the /etc/securetty file owned by root.	Check /etc/securetty ownership: # ls –lL /etc/securetty If /etc/securetty is not owned by root, then this is a finding.	The /etc/securetty file is owned by root.			
LINUX-SPECIFIC-23	AC-3, AC-6	Checks to see if the /etc/securetty file is more permissive than 640.	Check /etc/securetty permissions: # ls –lL /etc/securetty If /etc/securetty is more permissive than 640, then this is a finding.	The /etc/securetty file has permissions less than or equal to 640.			

IRS Safeguard SCSEM Legend

Test Case Tab: Execute the test cases and document the results to complete the IRS Safeguard Computer Security review. Reviewer is required to complete the following columns: Actual Results, Comments/Supporting Evidence.

Test ID	Identification number of SCSEM test case
NIST ID	NIST 800-53/PUB 1075 Control Identifier
Test Objective	Objective of test procedure.
Test Steps	Detailed test procedures to follow for test execution.
Expected Results	The expected outcome of the test step execution that would result in a Pass.
Actual Results	The actual outcome of the test step execution, i.e., the actual configuration setting observed.
Pass/Fail	Reviewer to indicate if the test case pass, failed or is not applicable.
Comments / Supporting Evidence	Reviewer to include any supporting evidence to confirm if the test case passed., failed on not applicable As evidence, provide the following information for the following assessment methods: 1. Interview - Name and title of the person providing information. Also provide the date when the information is provided. 2. Examination - Provide the name, title, and date of the document referenced as the evidence. Also provide section number where the pertinent information is resident within the document (if possible). Ensure all supporting evidence to verify the test case passed or failed. If the control is marked as NA, then provide appropriate justification as to why the control is considered NA.